Mineração de Bitcoins e o Uso da Tecnologia Blockchain

MCTA025-13 - Sistemas Distribuídos
Centro de Matemática, Computação e Cognição
Universidade Federal do ABC

1º de Agosto 2018

Emilio Francesquini
e.francesquini@ufabc.edu.br

Vladimir Rocha
vladimir.rocha@ufabc.edu.br

Disclaimer

UFABC

- Estes slides foram preparados para o curso de Sistemas Distribuídos na UFABC.

- Este material pode ser usado livremente desde que sejam mantidos, além deste aviso, os créditos aos autores e instituições.

- Estes slides foram adaptados daqueles originalmente preparados para a IV Semana do CMCC por E. Francesquini e V. Rocha.

Agenda

UFABC

- Bitcoin
- O que é Blockchain?
- Premissas
- Como funciona
- Arquiteturas
- Mineração de Bitcoin

O surgimento das criptomoedas

UFABC

- Criadas originalmente como uma promessa/alternativa às grandes corporações financeiras
  - Um sistema bancário sem uma entidade centralizadora
- Hoje é bem simples para qualquer um comprar, vender e minerar moedas virtuais
- Como qualquer tecnologia, logo começou a ser utilizada para fins, no mínimo, discutíveis
  - Governos preocupados com os usos ilícitos e a falta de uma entidade controladora
- Teve um grande sucesso pois surgiu aproximadamente ao mesmo tempo da crise de 2009

Bitcoin

UFABC

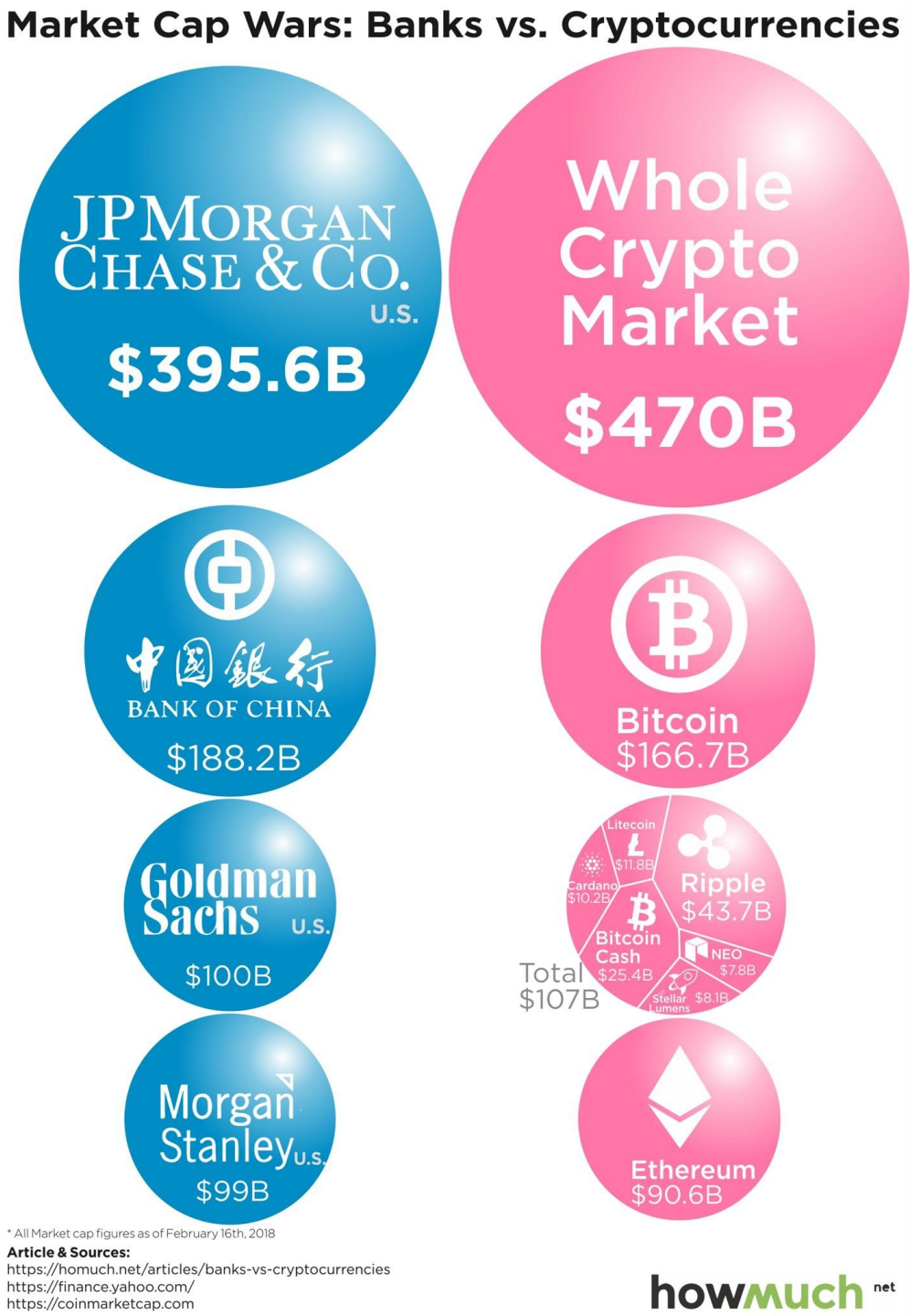
- Moeda virtual alternativa que surge em 2009
- Não atrelada a bancos ou governos
- Criadas através de um processo computacional
- As transações são realizadas entre pessoas anônimas (sem intermediários)
- Tão anônimo que até hoje não se sabe quem é Satoshi Nakamoto

Atualmente existem mais de 1600 moedas virtuais parecidas ao Bitcoin!

https://coinmarketcap.com/pt-br/

Valor de Mercado

- O valor de mercado do Bitcoin atualmente ultrapassa o PIB de Marrocos
  - Contudo é importante levar em consideração as violentas mudanças de cotação típicas das criptomoedas
- Comparado aos maiores bancos do Brasil (Market Cap):
  - Mercado de criptomoedas - US$ 470B
  - Bitcoin - US$ 166B
  - Itaú Unibanco - US$ 71B
  - Bradesco - US$ 49B
- Também há roubo a bancos
  - Coincheck US$ 530M
  - Mt. Gox US$470M



O que é Blockchain?

UFABC

- Blockchain é uma tecnologia que permite registrar as transações realizadas entre as pessoas de forma anônima, imutável, transparente e descentralizada.

- Todas as moedas virtuais (criptomoedas) estão baseadas nessa tecnologia.

Premissas do Blockchain

- Blockchain é uma tecnologia que permite registrar as transações realizadas entre as pessoas de forma anônima, imutável, transparente e descentralizada

- Autenticidade
- Anonimato
- Imutabilidade
- Transparência
- Tolerância a falhas

Premissas: Autenticidade

- Assinatura Digital que substitui a assinatura física.
- É possível confirmar que a assinatura foi feita pelo dono (não repúdio).
- Evita alterações ao documento assinado (integridade).

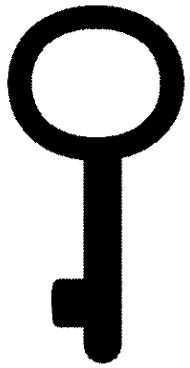


Imagem: http://acime.com.br/v6/noticias/acime-celebra-um-ano-de-certificacao-digital

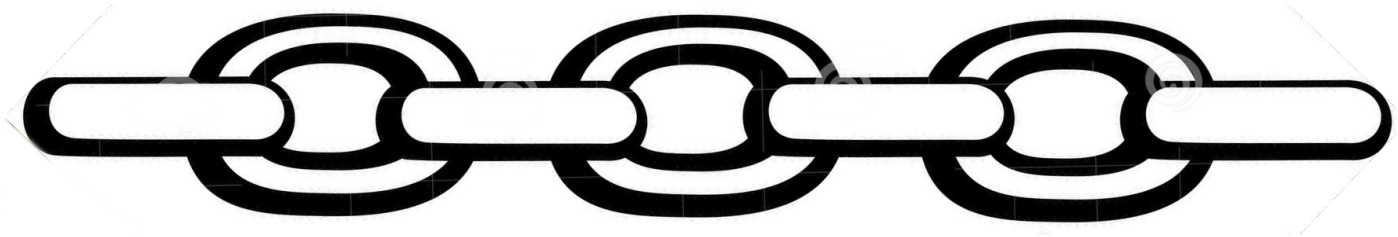
Premissas: Anonimato

- A diferença de um e-CPF, não é necessário saber quem é a dona ou dono
  - Em outras palavras, a pessoa fica anônima
- Porém, as características da autenticidade (não repúdio e integridade) se mantêm

Imagem: http://bitcoincardcomparison.com/anonymous-cards/

Premissas: Imutabilidade

- Uma vez que a transação for autenticada e registrada, ninguém poderá mudá-la
- Intuitivamente pense em que cada elo é uma transação e está encadeada com outra



Premissas: Transparência

- Como as transações são autênticas e imutáveis, podem ser rastreadas e auditadas
- Mas, dado o anonimato, não será possível saber quem é a dona

Imagem: https://www.pwc.co.uk/issues/futuretax/how-blockchain-technology-could-improve-tax-system.html

Premissas: Tolerância a Falhas

- Todos os donos (i.e., computadores) possuem a mesma cadeia de transações.
- Se um sair da rede, a cadeia não será perdida.

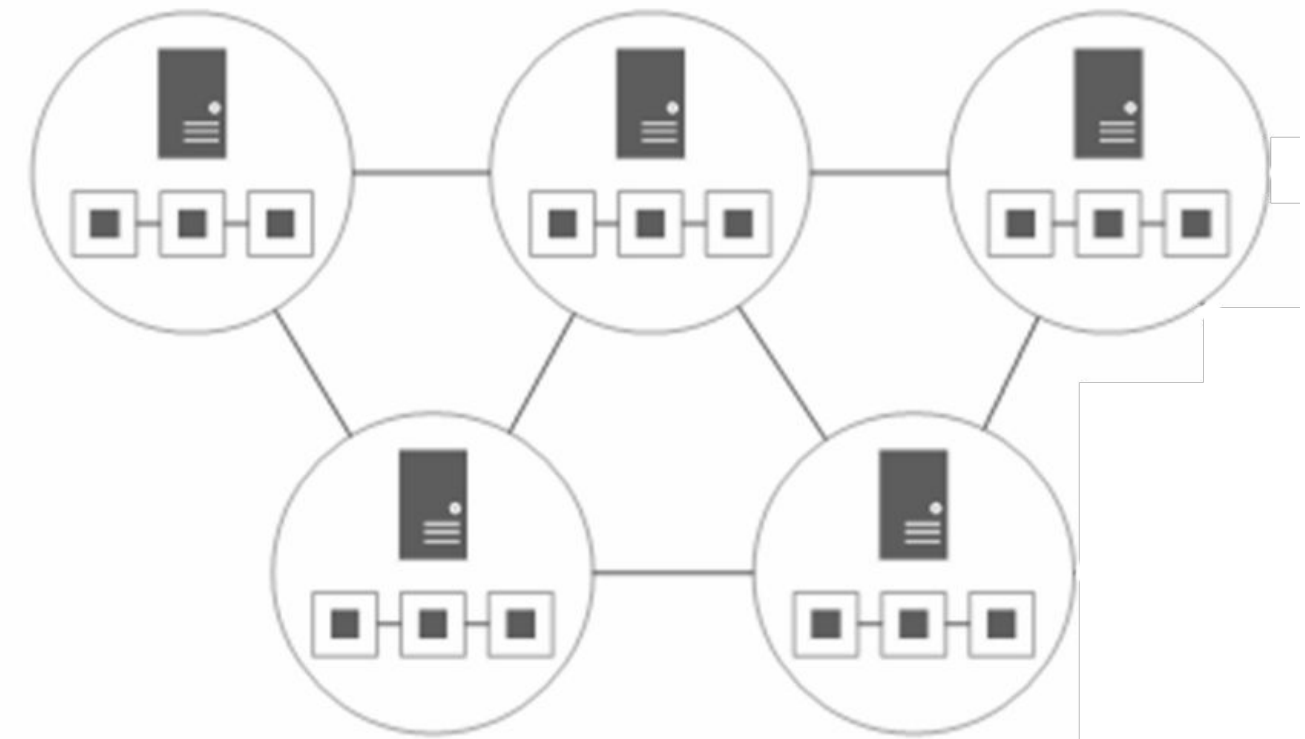


Imagem: https://medium.com/@vdenotaris/how-i-did-implement-my-first-blockchain-network

Como funciona o Blockchain?

UFABC

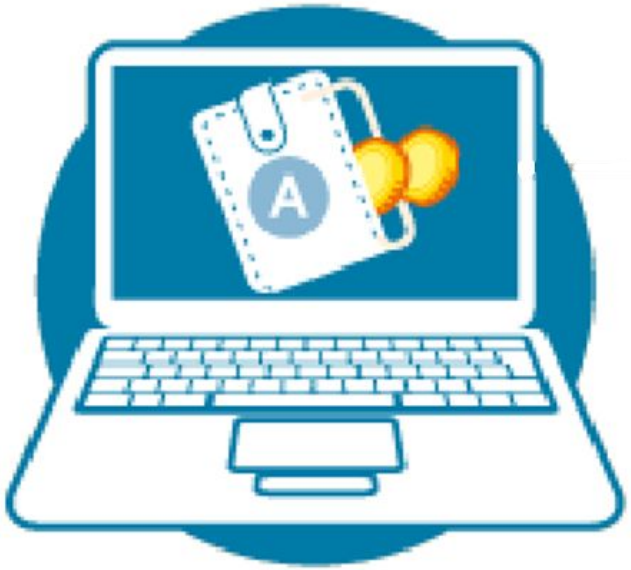
- Visão geral
- Assinatura Digital
- Transação
- Bloco
- Consenso

Como funciona: Visão Geral

1. Dono “A” quer realizar uma transação

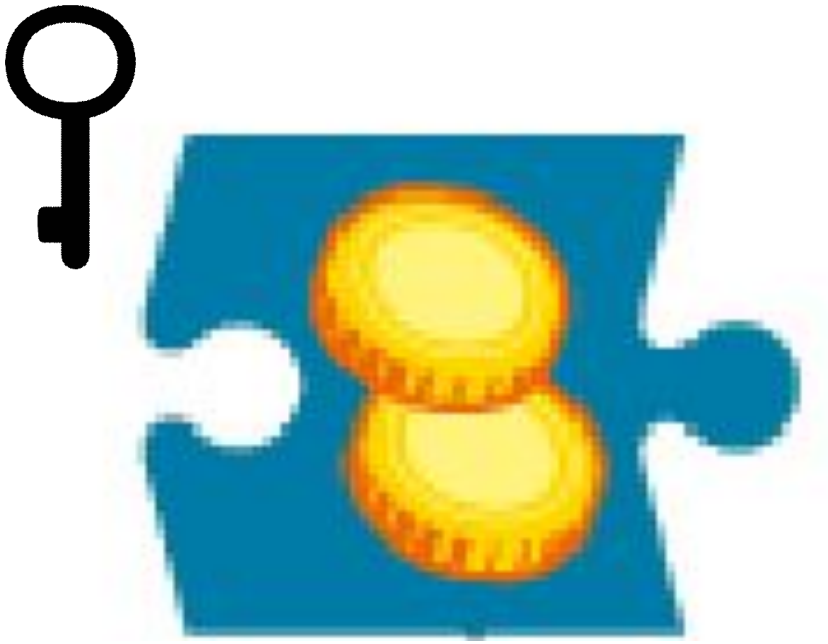
Exemplos:

- Envio de dinheiro de A para B
- Certidão de posse de uma casa
- Registro de um prontuário médico



Como funciona: Visão Geral

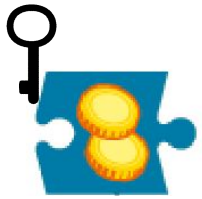
2. A transação é assinada por “A” é associada a um “bloco”



Como funciona: Visão Geral

UFABC

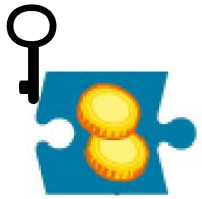
3. O bloco é transmitido a todos os membros da rede

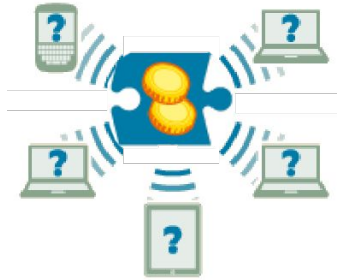


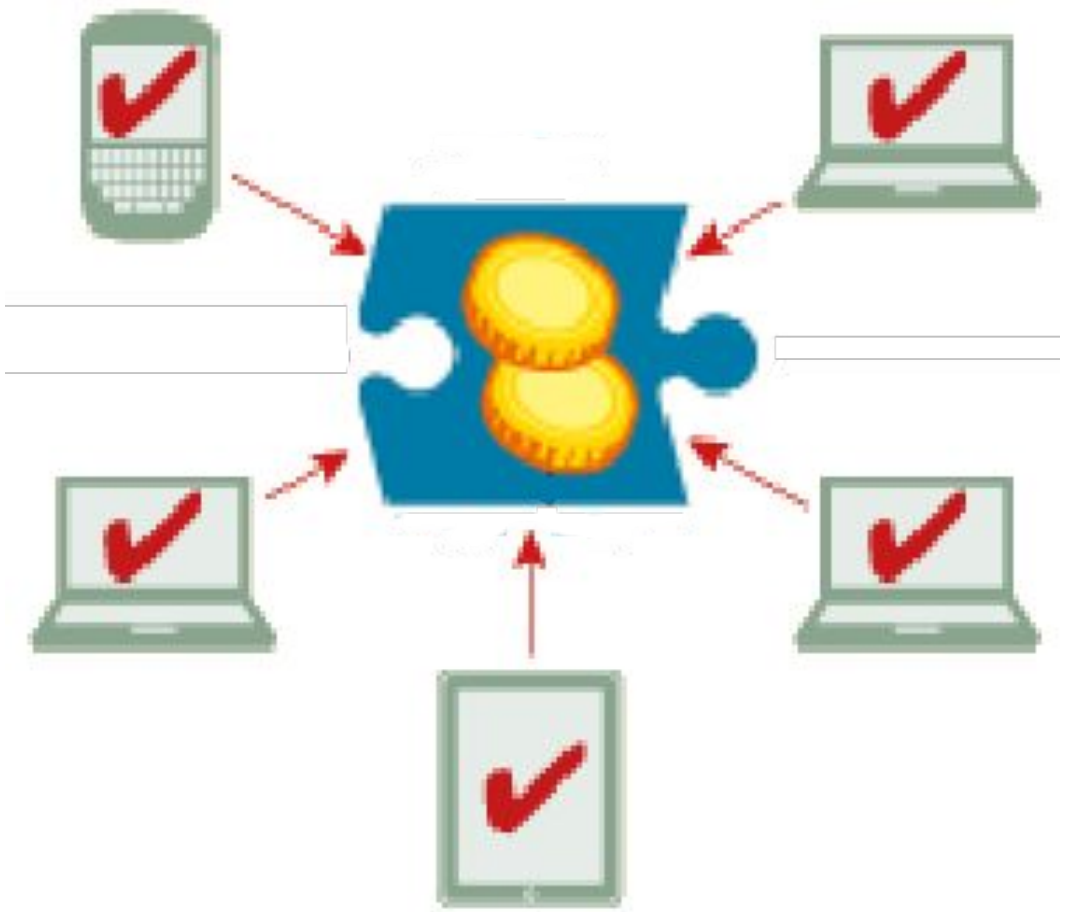
Como funciona: Visão Geral

UFABC

4. Os membros da rede aprovam o bloco (e a transação) como válido

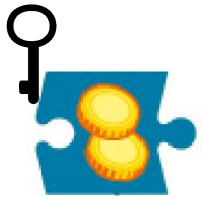
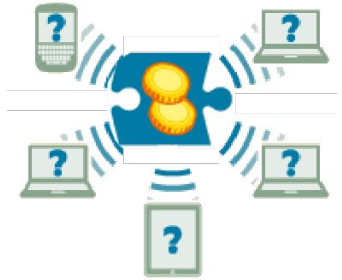
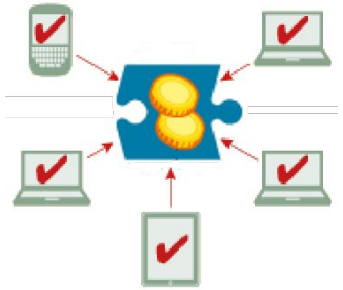
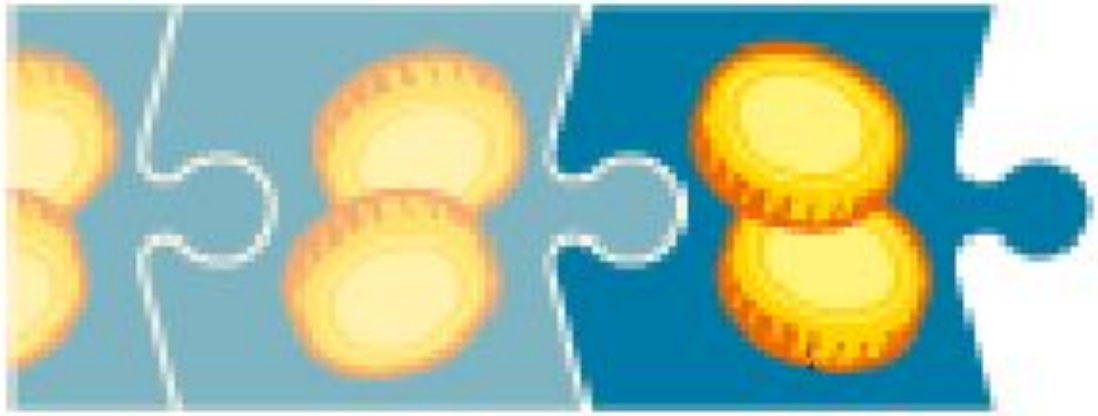






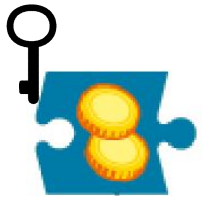
Como funciona: Visão Geral

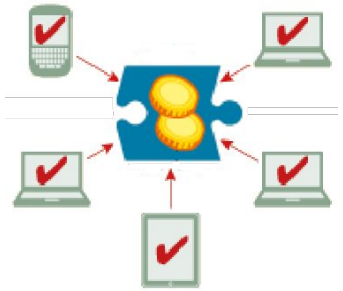
4. O bloco é adicionado à cadeia

Como funciona: Visão Geral

4. Dono “B” recebe (e pode corroborar) o dinheiro





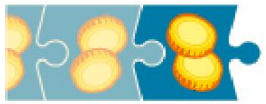


Imagem: Fonte FT – Insider PRO

Como funciona o Blockchain?

UFABC

- Visão geral
- Assinatura Digital
- Transação
- Bloco
- Consenso

Como funciona: Assinatura

- Transformação da mensagem (*hash*) ~ marca d'água ~ integridade

Imagem: https://criptonoticias.com.br/o-que-e-uma-cadeia-de-blocos-block-chain/

Como funciona: Assinatura

- Transformação da mensagem (*hash*) ~ marca d'água ~ integridade

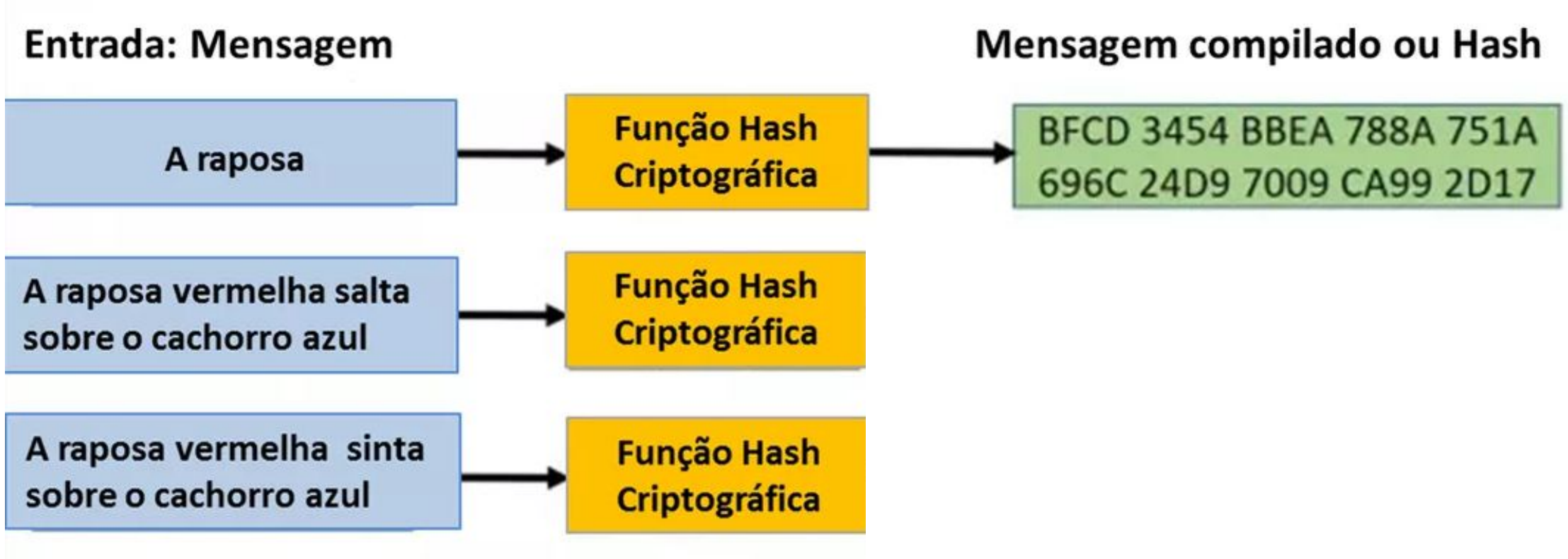


Imagem: https://criptonoticias.com.br/o-que-e-uma-cadeia-de-blocos-block-chain/

Como funciona: Assinatura

- Transformação da mensagem (*hash*) ~ marca d'água ~ integridade

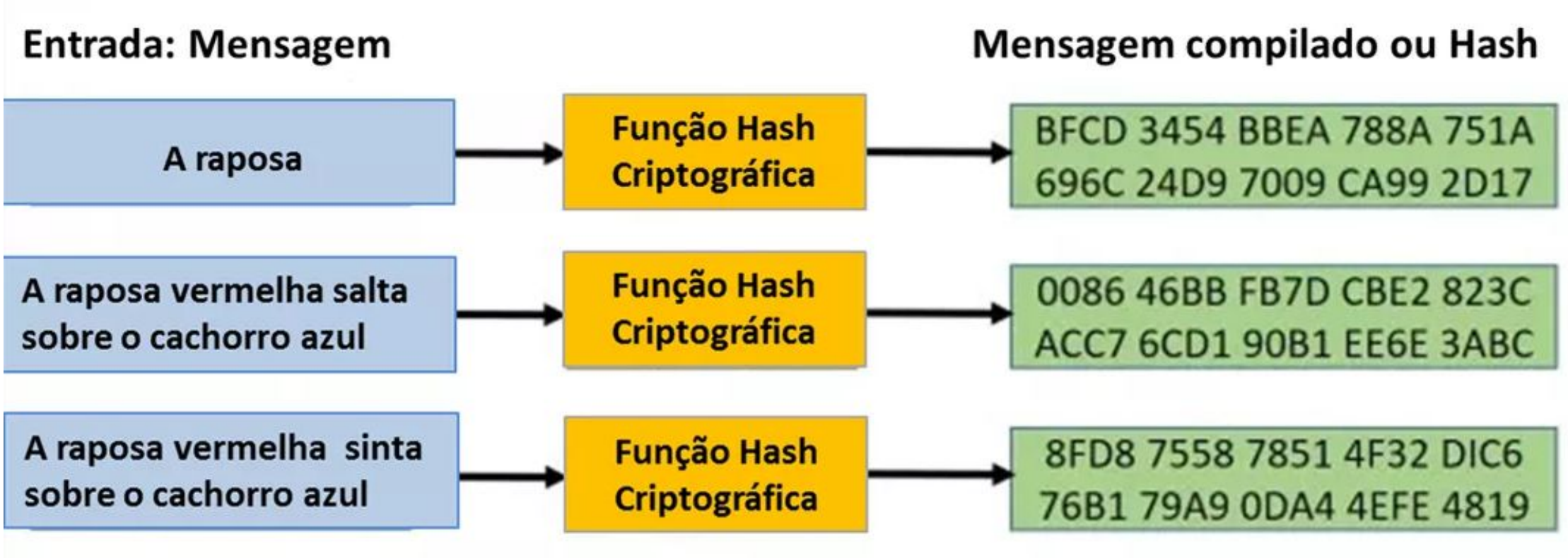
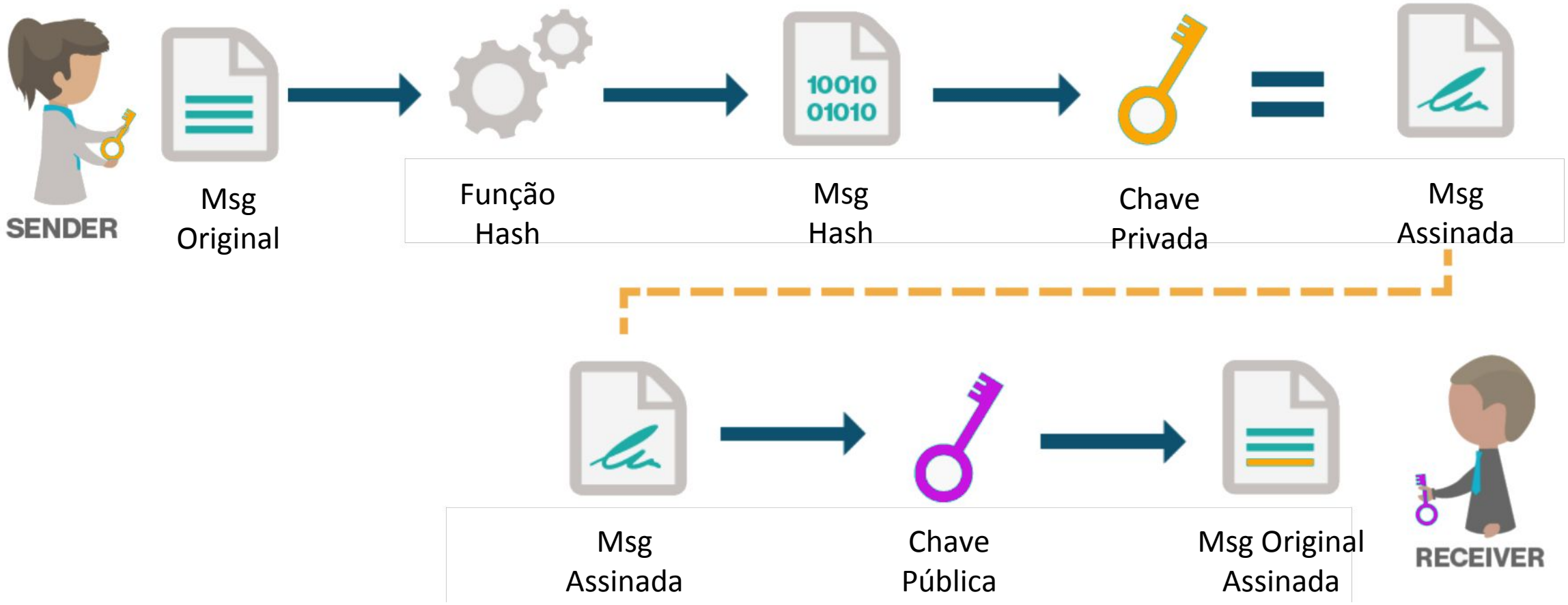


Imagem: https://criptonoticias.com.br/o-que-e-uma-cadeia-de-blocos-block-chain/

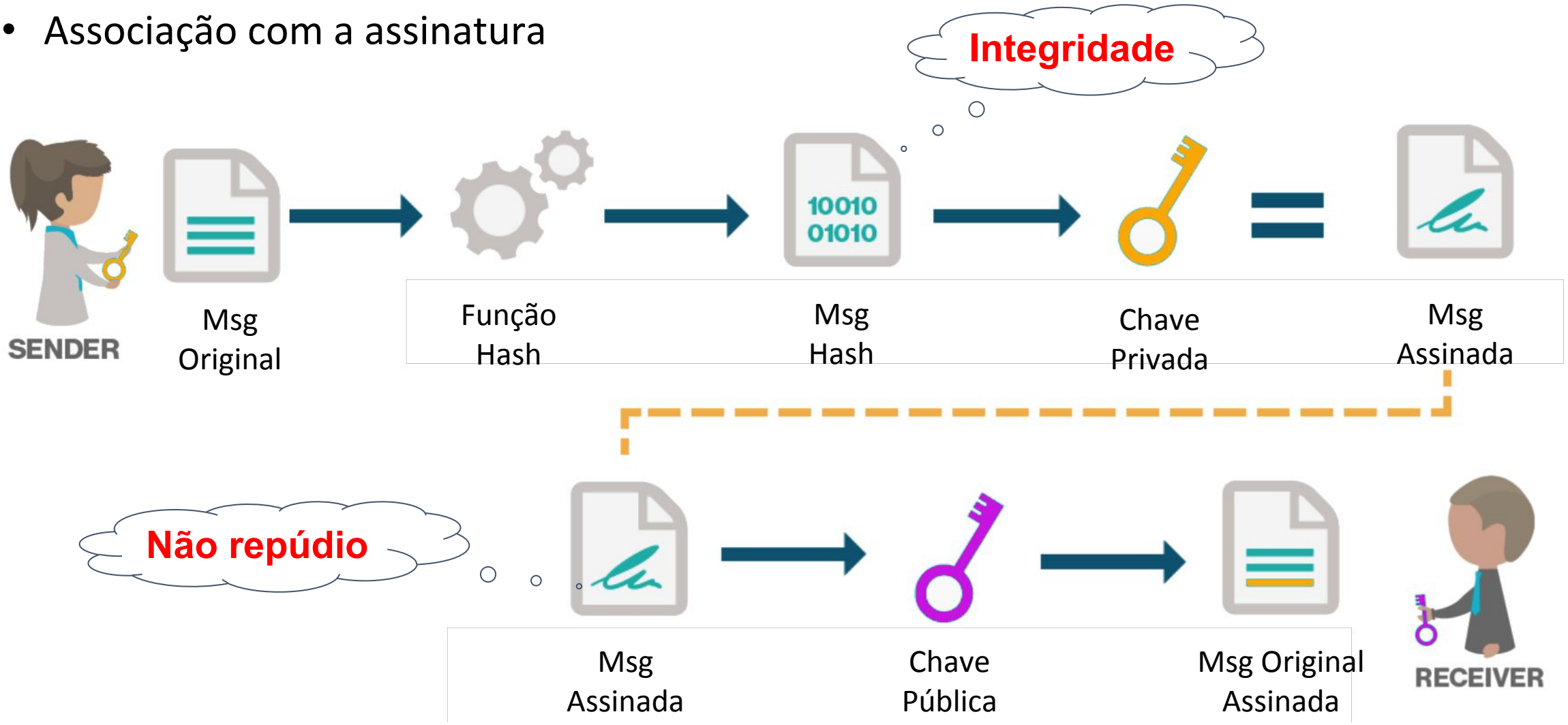
Como funciona: Assinatura Digital

- Associação com a assinatura



Como funciona: Assinatura Digital

- Associação com a assinatura

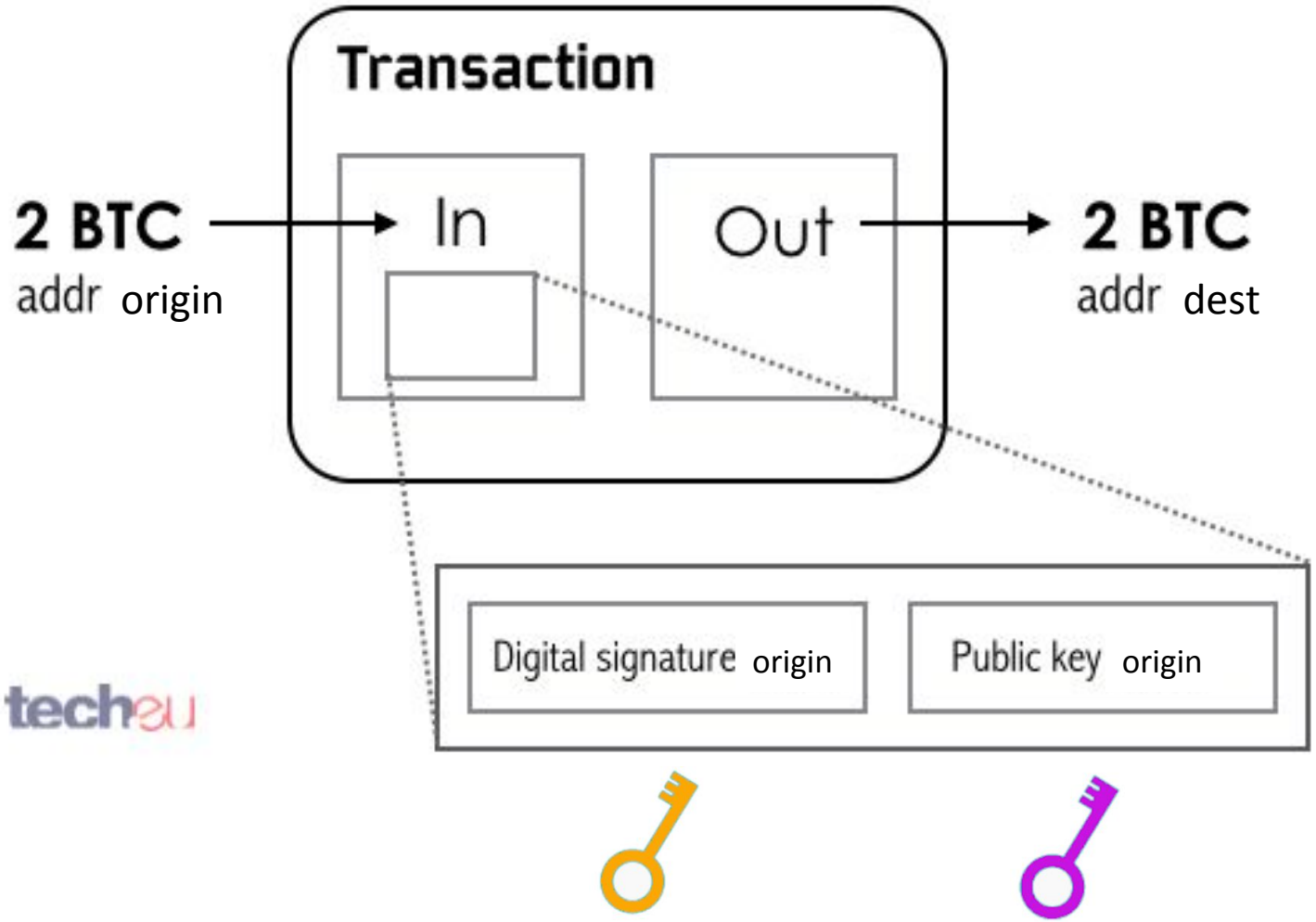


Como funciona o Blockchain?

UFABC

- Visão geral
- Assinatura Digital
- Transação
- Bloco
- Consenso

Como funciona: Transação

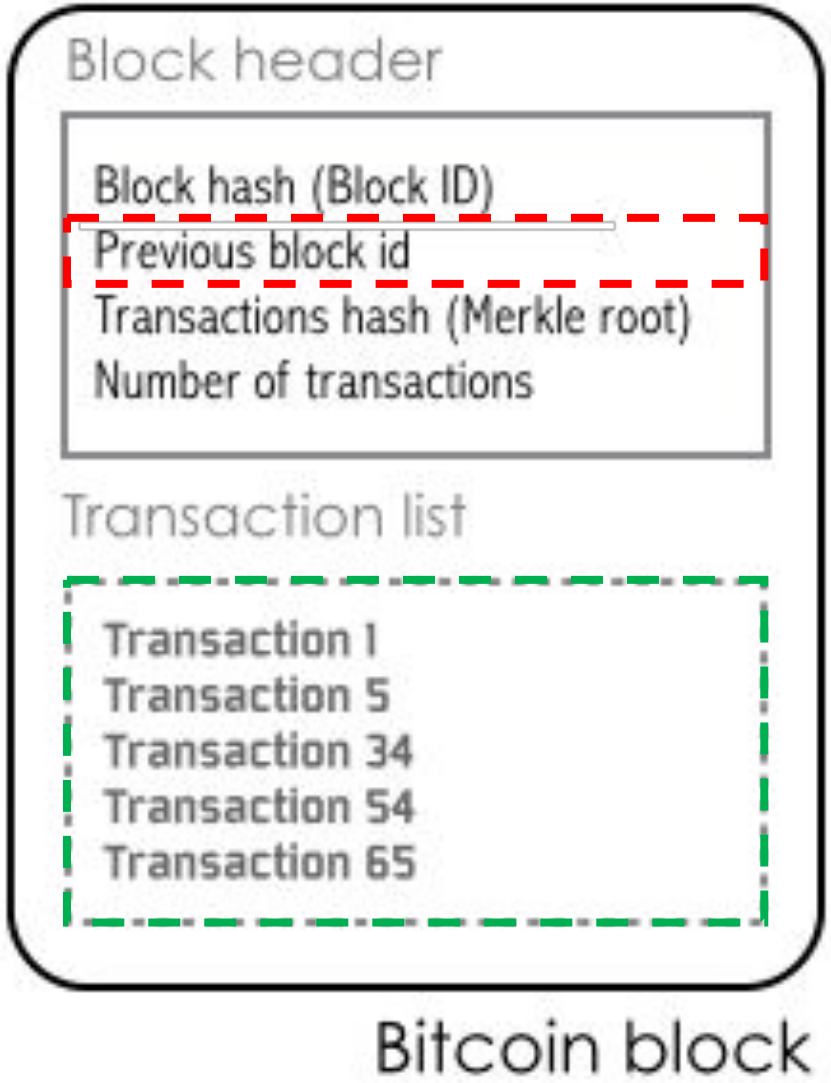


Como funciona o Blockchain?

UFABC

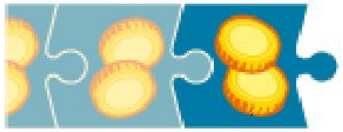
- Visão geral
- Assinatura Digital
- Transação
- Bloco
- Consenso

Como funciona: Bloco



https://blockexplorer.com/

Como funciona: Bloco



UFABC

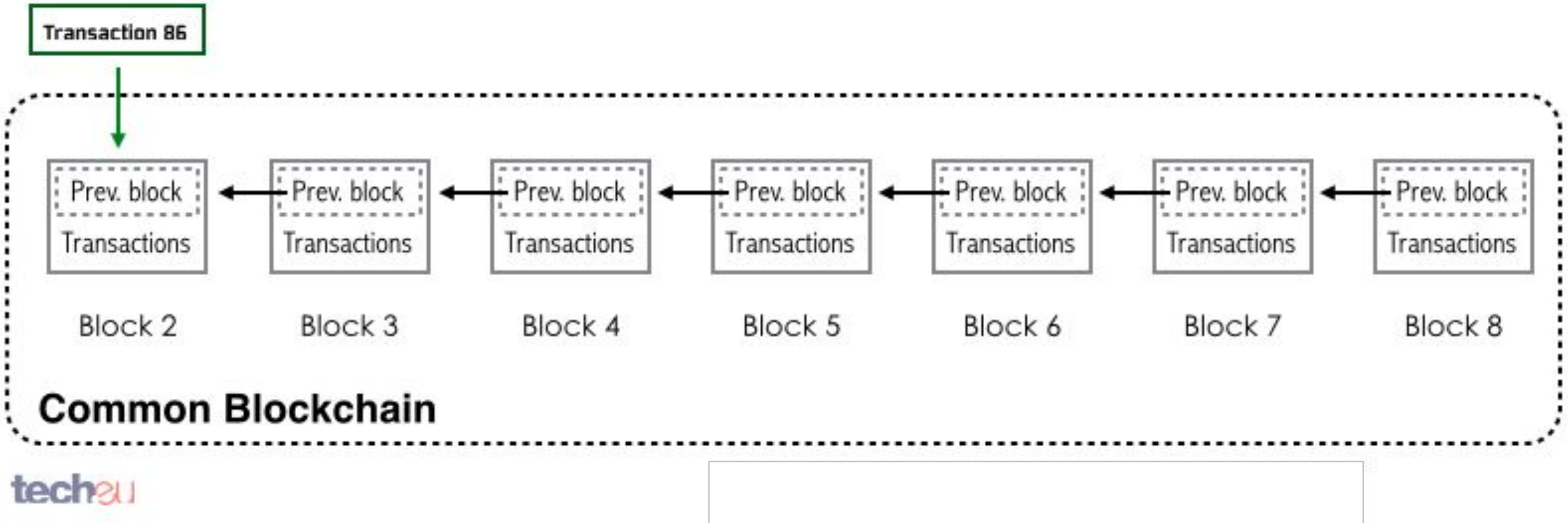
Como se adiciona um novo bloco na cadeia?

- Um membro da rede deve resolver um problema matemático complexo associado ao novo bloco (*proof-of-work PoW*)

- Quando resolvido, o membro adiciona o novo bloco à cadeia e dissemina essa informação aos outros membros.

Como funciona: Cadeia de Blocos

UFABC



techeu

Como funciona o Blockchain?

UFABC

- Visão geral
- Assinatura Digital
- Transação
- Bloco
- Consenso

Como funciona: Consenso

Quando resolvido (o problema matemático), o membro adiciona o novo bloco à cadeia e dissemina essa informação aos outros membros.

Imagem: https://medium.com/@micheledaliessi/how-does-the-blockchain-work-98c8cd01d2ae

Como funciona: Consenso

- Que acontece se vários membros resolvem o problema matemático e disseminam o bloco ao mesmo tempo?
- Em outras palavras, como geramos o consenso de qual bloco usar?

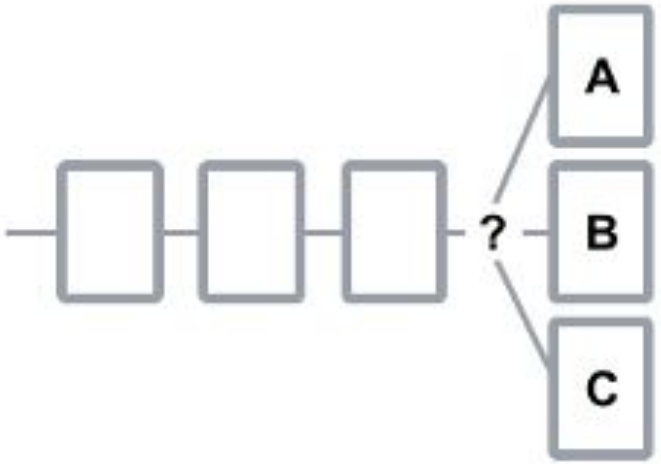


Imagem: https://medium.com/@micheledaliessi/how-does-the-blockchain-work-98c8cd01d2ae

Como funciona: Consenso

- Regra: cada nó utilizará sempre a cadeia mais longa disponível

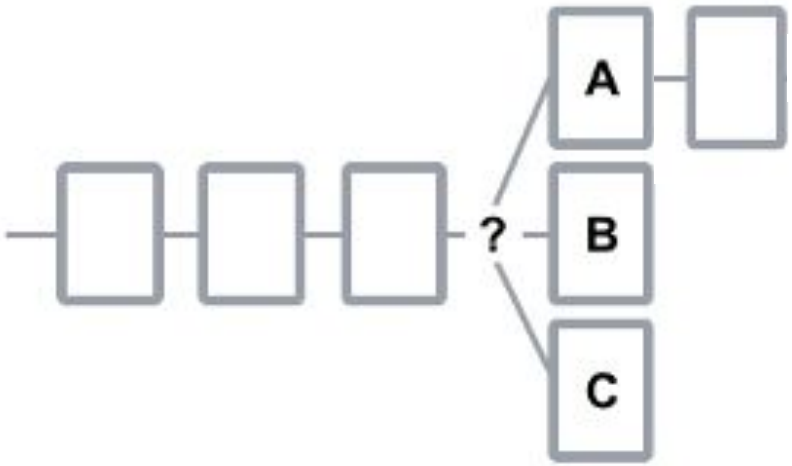


Imagem: https://medium.com/@micheledaliessi/how-does-the-blockchain-work-98c8cd01d2ae

Como funciona: Consenso

- Regra: cada nó utilizará sempre a cadeia mais longa disponível

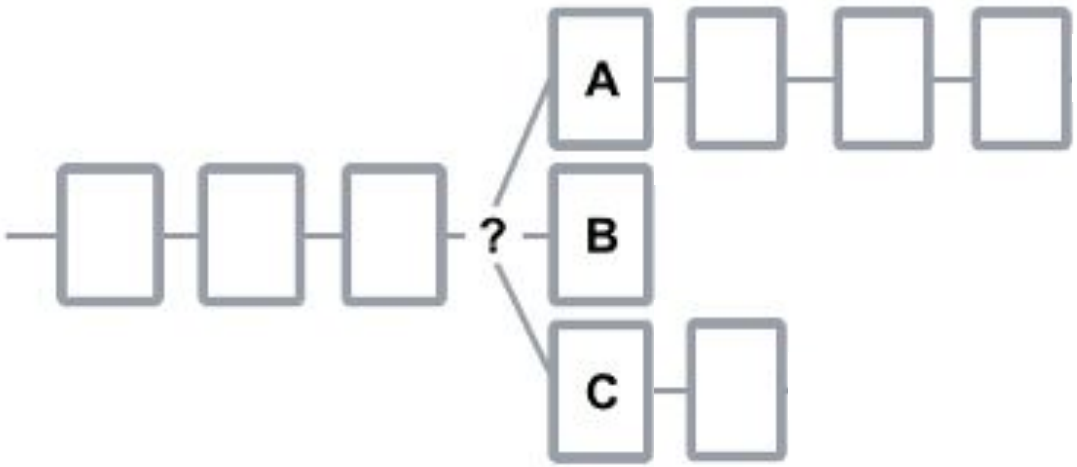


Imagem: https://medium.com/@micheledaliessi/how-does-the-blockchain-work-98c8cd01d2ae

Como funciona: Consenso

- Regra: cada nó utilizará sempre a cadeia mais longa disponível

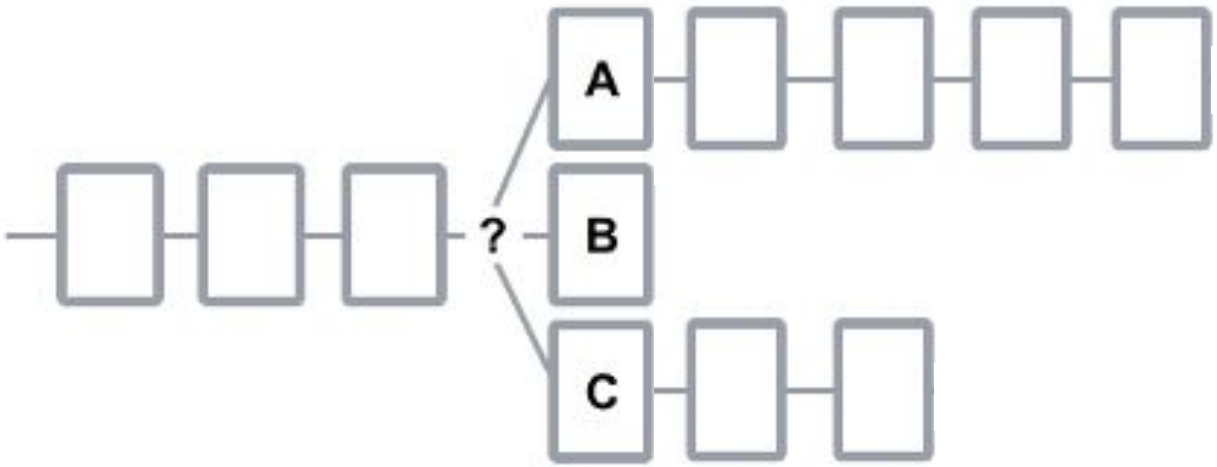


Imagem: https://medium.com/@micheledaliessi/how-does-the-blockchain-work-98c8cd01d2ae

Como funciona: Consenso

- Regra: cada nó utilizará sempre a cadeia mais longa disponível
- Em “algum momento” B e C receberão a cadeia de A, abandonando as suas e assimilando a de A

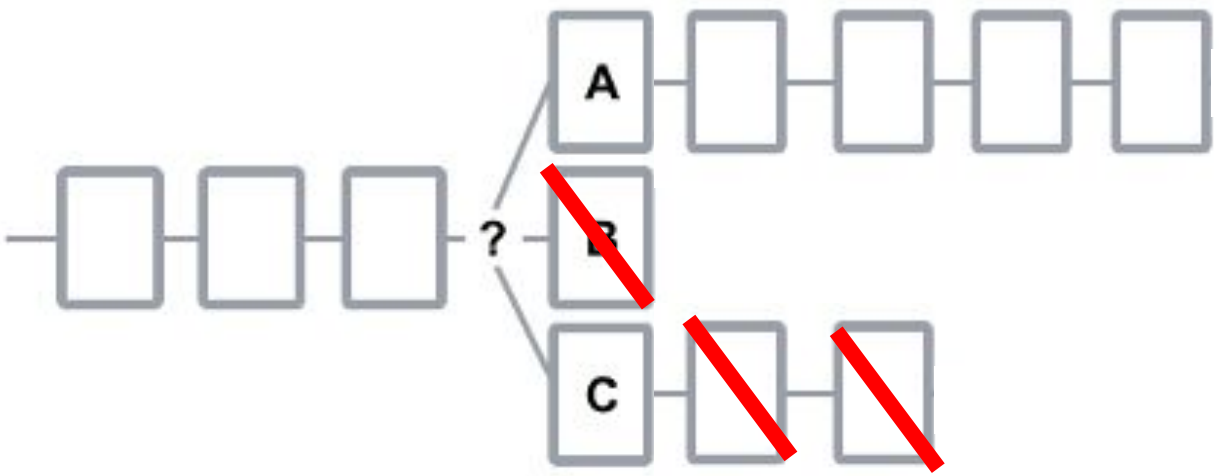


Imagem: https://medium.com/@micheledaliessi/how-does-the-blockchain-work-98c8cd01d2ae

Arquiteturas

UFABC

- Existem dezenas de implementações do blockchain.
- Qual usar?

1. Propósito
2. Modo de participação
3. Quem controla as decisões
4. Desempenho

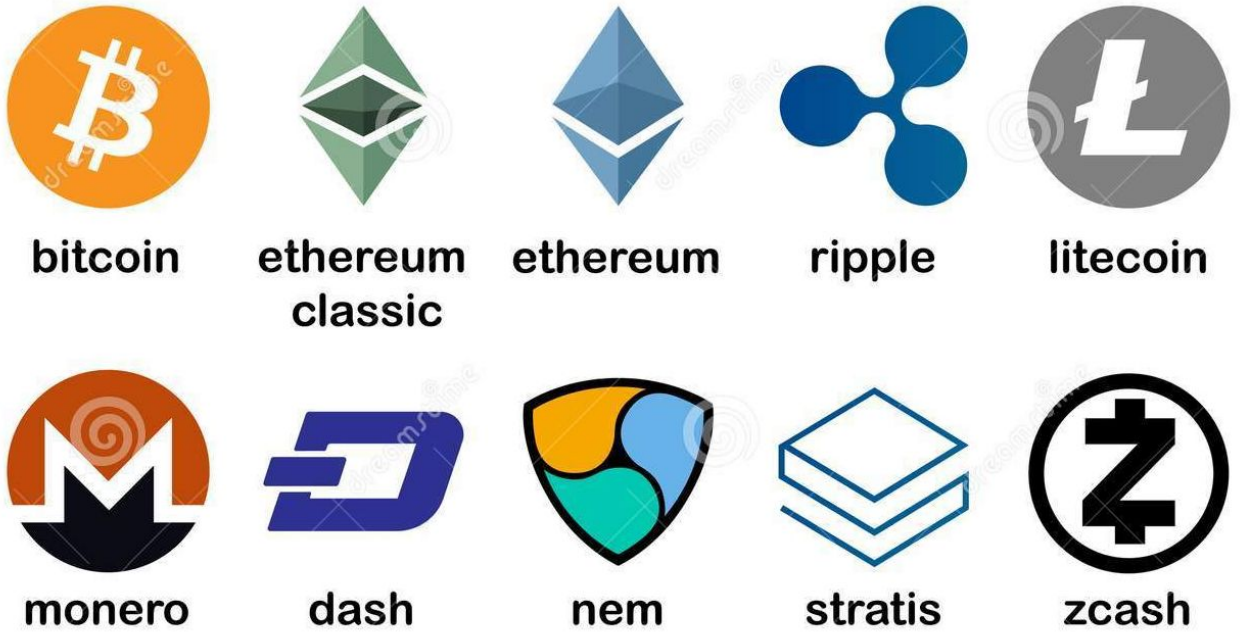


Imagem: https://dreamtime.com

Arquiteturas

UFABC

09/2012	07/2015	12/2015	03/2016	07/2017
Bitcoin	Ethereum	Hyperledger	Steem	Filecoin

Arquiteturas

UFABC

1. Propósito: para que foi criado inicialmente o blockchain?

09/2012	07/2015	12/2015	03/2016	07/2017
Bitcoin	Ethereum	Hyperledger	Steem	Filecoin
Criptomoedas	Uso geral + DApps	Uso geral + DApps	Rede social	HD Distribuído

Arquiteturas

UFABC

1. Propósito: para que foi criado inicialmente esse blockchain?
2. Modo de participação: aberto ou precisa de registro

09/2012	07/2015	12/2015	03/2016	07/2017
Bitcoin	Ethereum	Hyperledger	Steem	Filecoin
Criptomoedas	Uso geral + DApps	Uso geral + DApps	Rede social	HD Distribuído
Aberto	Aberto	Prova de identidade	Aberto	Aberto

Arquiteturas

UFABC

3. Quem controla as decisões

09/2012	07/2015	12/2015	03/2016	07/2017
Bitcoin	Ethereum	Hyperledger	Steem	Filecoin
Criptomoedas	Uso geral + DApps	Uso geral + DApps	Rede social	HD Distribuído
Aberto	Aberto	Prova de identidade	Aberto	Aberto
A rede	A rede	Autoridades	Não é claro	A rede

Arquiteturas

3. Quem controla as decisões
4. Desempenho

09/2012	07/2015	12/2015	03/2016	07/2017
Bitcoin	Ethereum	Hyperledger	Steem	Filecoin
Criptomoedas	Uso geral + DApps	Uso geral + DApps	Rede social	HD Distribuído
Aberto	Aberto	Prova de identidade	Aberto	Aberto
A rede	A rede	Autoridades	Não é claro	A rede
7 tx/s	Sem limite (10)	10.000 tx/s (1000)	10.000 tx/s	Não é claro

Mineração de Bitcoin

- O que exatamente significa minerar?
  - Cálculo do hash do bloco calculado usando SHA-256 levando em conta a dificuldade atual (atualizada dinamicamente) da rede
  - Mineração está mais para adivinhação do que para resolução
  - Recompensa (atualmente 12.5 BTC) para quem encontrar a solução primeiro

Height	Time	Relayed By	Hash	Size (kB)
528051 (Main Chain)	2018-06-18 11:19:33	BTC.TOP	0000000000000000001b704af44ac2b63f59948de276f181ab4a3dbe2e37a080	803
528050 (Main Chain)	2018-06-18 11:10:10	F2Pool	0000000000000000037497d7dffdbbb69f70d3d59f438e7d2239c107195fec8	664.91
528049 (Main Chain)	2018-06-18 11:08:52	F2Pool	0000000000000000000ccb9f131074d1ab3e8bd62a33844736c3cbfd71e02f2b	1,170.68
528048 (Main Chain)	2018-06-18 10:42:42	BitClub Network	0000000000000000019dded40f072c08f0b3ec453134e6b2f952451848188e4	184.28
528047 (Main Chain)	2018-06-18 10:39:33	Unknown	00000000000000000006755955b7f17625af22386c18989d0124552892767472	486.31
528046 (Main Chain)	2018-06-18 10:32:30	ViaBTC	0000000000000000000108e0bd29d1a9cfcbf503f0430c0af47190ca89bfaf08d	389.72
528045 (Main Chain)	2018-06-18 10:28:50	BTC.com	0000000000000000002ea2de35934f6d0a3d63a3bfac9702eae510da85eda4da	354.38

Mineração de Bitcoin

UFABC

Resumo	
Altura	528049 (Main chain)
Jogo da velha	0000000000000000000ccb9f131074d1ab3e8bd62a33844736c3cbfd71e02f2b
Bloco Anterior	0000000000000000019dded40f072c08f0b3ec453134e6b2f952451848188e4
Próximos Blocos	00000000000000000037497d7dffdbbb69f70d3d59f438e7d2239c107195fec8
Hora	2018-06-18 11:08:52
Transmitido Em	2018-06-18 11:08:52
Enviado Por	F2Pool
Dificuldade	4,940,704,885,521.83
Bits	389609537
Número de Transações	2270
Total de Saída	17,831.90207363 BTC
Valor Estimado de Transações	656.5932441 BTC
Tamanho	1170.685 KB
Versão	0x20000000
Merkle Root	6fb3f05a2368c097fa0491be720b61f87bdb6f1ab868f242e85575ec6c0b25e9
Nonce	3229975828
Recompensa pelo Bloco	12.5 BTC
Taxas de Transação	0.30484879 BTC

Mineração de Bitcoin

UFABC

Resumo	
Altura	528049 (Main chain)
Jogo da velha	0000000000000000000ccb9f131074d1ab3e8bd62a33844736c3cbfd71e02f2b
Bloco Anterior	0000000000000000019dded40f072c08f0b3ec453134e6b2f952451848188e4
Próximos Blocos	00000000000000000037497d7dffdbbb69f70d3d59f438e7d2239c107195fec8
Hora	2018-06-18 11:08:52

Nonce	3229975828
Recompensa pelo Bloco	12.5 BTC
Taxas de Transação	0.30484879 BTC

Valor Estimado de Transações	656.5932441 BTC
Tamanho	1170.685 KB
Versão	0x20000000
Merkle Root	6fb3f05a2368c097fa0491be720b61f87bdb6f1ab868f242e85575ec6c0b25e9

Nonce	3229975828
Recompensa pelo Bloco	12.5 BTC
Taxas de Transação	0.30484879 BTC

Mineração de Bitcoin - CPUs

UFABC

- A ideia original de se utilizar PoW visava dar igual poder de voto a todos os participantes da rede: “1 CPU = 1 VOTO”
- E a mineração começou exatamente assim, com CPUs

CPU	Mining speed (KH/s)	Power used (Watts)	# of cores
Athlon 64 X2 5600+	6.07	89	2
Athlon II X3 425	9.5	125	4
Phenom II X4 955	22	125	4
FX-8120	46	125	8
FX-8350	65	125	8
Core 2 Quad Q6600	9.68	100	4
Core 2 Quad Q9550	32.2	125	4
Core i3-2130	23	65	4
Core i5-2500K	48	90	4
Core i5-3570K	55	90	4
Core i7-3930K	98	200	12

Mineração de Bitcoin - GPUs

UFABC

- Oferecem um grau de paralelização muito maior do que CPUs

GPU	Mining speed (MH/s)	Power used (Watts)
AMD 4870	90	150
AMD 5770	240	100
AMD 5830	300	125
AMD 5850	400	180
AMD 5870	480	200
AMD 5970	800	350
AMD 6990	800	400
NVIDIA GT-210	4	30
NVIDIA GTX-280	60	230
NVIDIA GTX-480	140	250
NVIDIA Tesla S1070	155	800
NVIDIA Tesla S2070	750	900

Mineração de Bitcoin - FPGAs

UFABC

- Circuitos desenhados exclusivamente para calcular SHA-256 (e nada mais!)

FPGA	Mining speed MH/s	Power used watts	Efficiency W/MH/s
Bitcoin Dominator X5000	100	6.8	0.068
Icarus	380	19.2	0.051
Lancelot	400	26	0.065
ModMiner Quad	800	40	0.05
Butterflylabs Mini Rig	25,200	1250	0.05

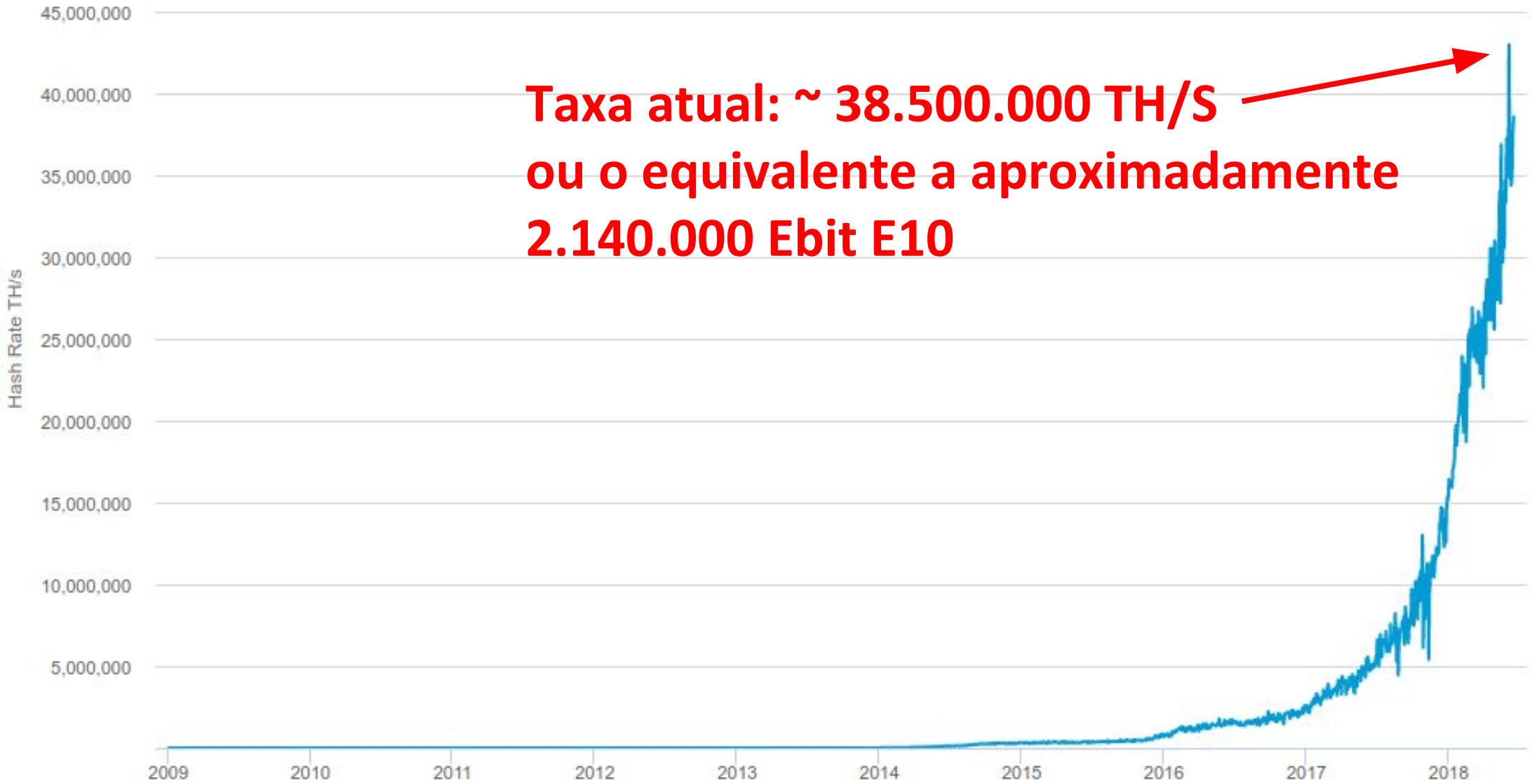
Mineração de Bitcoin - ASICs

UFABC

- Mais eficientes que FPGAs...
- ...e muito mais baratos!

ASIC	MH/s	Watts	MH/J
Ebit E10	18.000.000	1620	11.111
Ebit E9++	14.000.000	1330	10.526
AntMiner S9	14.000.000	1375	10.181
Avalon821	11.000.000	1200	9.166
Ebit E9+	9.000.000	1300	6.923

Qual o retorno esperado?



Taxa atual: ~ 38.500.000 TH/S
ou o equivalente a aproximadamente
2.140.000 Ebit E10

Qual o retorno esperado?

UFABC

- Vamos considerar
  - Média de 10 minutos por bloco, 6 por hora, 144 por dia
  - Prêmio atual por bloco descoberto: 12.5 BTC
  - Média de taxas de transação: 0.5 BTC
  - Rede: 38.500.000 TH/s
  - Custo da energia: **Grátis!**
  - Cotação do Dólar/BTC: US$ 6450

Qual o retorno esperado?

UFABC

	Hash Speed (TH/s)	%	BTC/Dia	US$/Dia	Preço (US$)	Break Even
Core i7-3930K	0,0000001	0,0000000000003	0,000000000005	0,00000003	160	13.977.267,88
AMD Radeon HD 6990	0,0008650	0,0000000022468	0,000000042059	0,00027128	250	2.524,80
Butterflylabs Mini Rig	0,0252	0,0000000654545	0,000001225309	0,00790324	15295	5.302,14
Ebit E10	18	0,0000467532468	0,000875220779	5,64517403	2800	1,36

Quão otimista é essa estimativa?

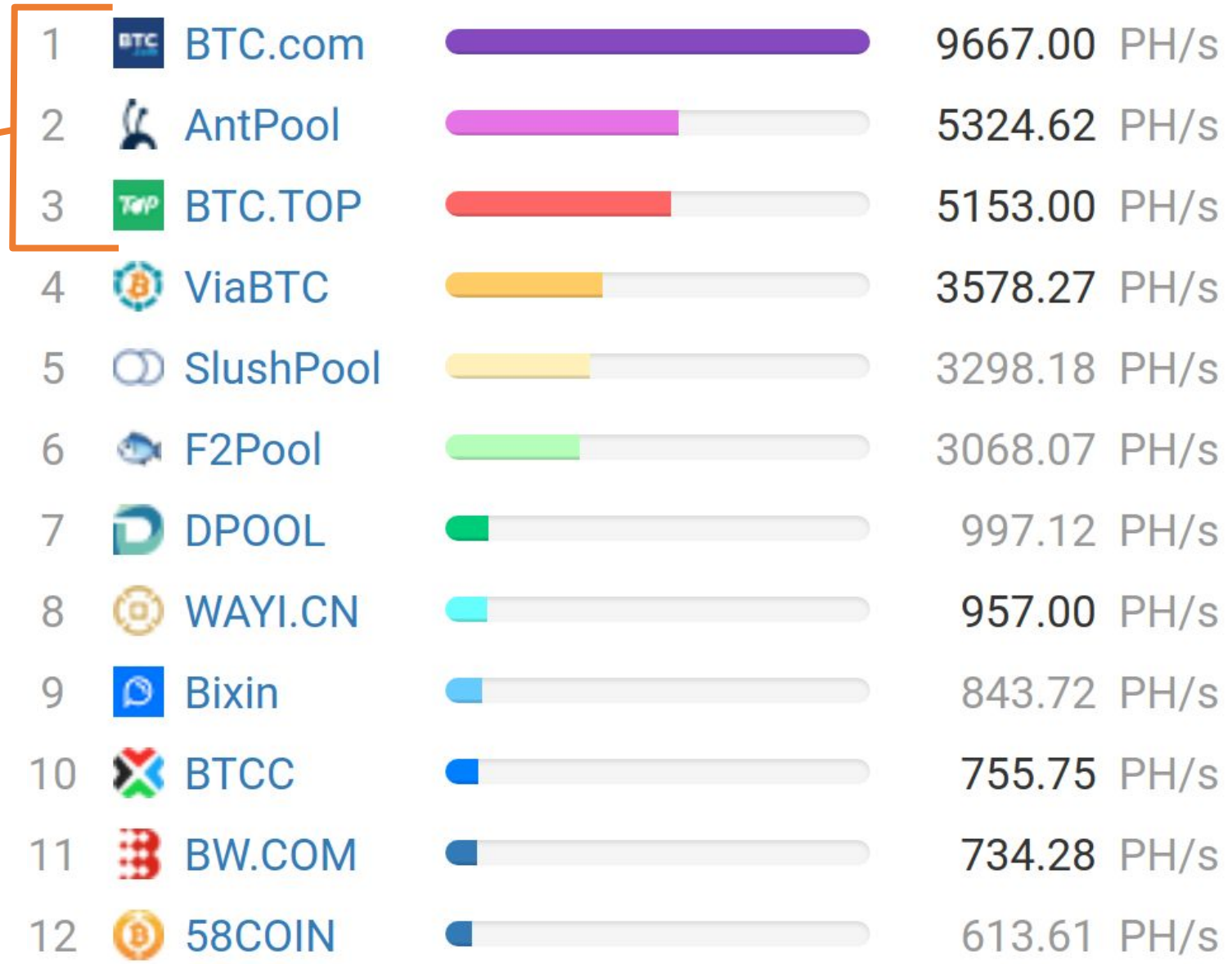
UFABC

- Assume que há uma distribuição igualitária entre os participantes
- Assume que o usuário, por conta, vai ter a sorte de encontrar um bloco
  - São suposições irreais na prática
- Isso levou usuários a formarem **pools de mineração**
  - Usuários compartilham o trabalho e as recompensas
  - Tipicamente o organizador cobra um % dos ganhos
  - Permite que mesmo pequenos mineradores consigam algum retorno

Pools de mineração

UFABC

Aproximadamente
53% da rede



Mineração Profissional

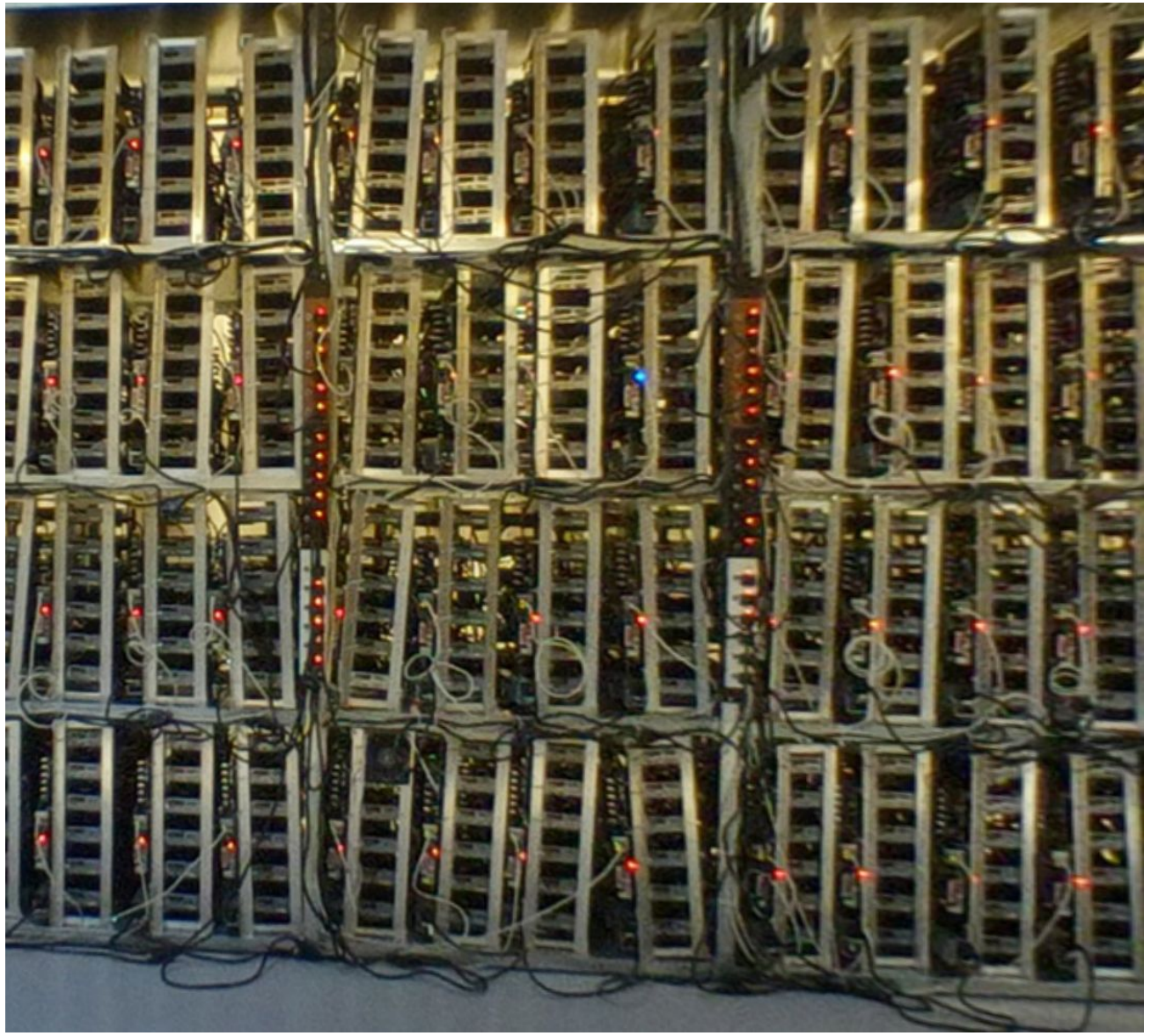
UFABC

- Alguns fabricantes perceberam que é mais lucrativo fabricar ASICs para “consumo próprio” do que vendê-los
- Já outros vendem o processamento no melhor estilo Cloud Computing
- Há muita especulação sobre a atual tecnologia empregada pelos mineradores profissionais
  - O vazamento de um segredo pode custar milhões!
  - Sabe-se contudo que diversos já utilizam ASICs com tecnologia de 16 nm
    - Para se ter uma ideia, a Intel passou do processo de 22 nm para 14 nm apenas em 2014!
- Há dados públicos sobre data centers de mineração consumindo de 0,5 a 5MW e planos para centros de mineração até 100MW
  - O computador mais rápido do mundo, o Sunway TaihuLight com 10.649.600 cores consome “apenas” ~15MW

Mineração Profissional

UFABC

Mineração Profissional

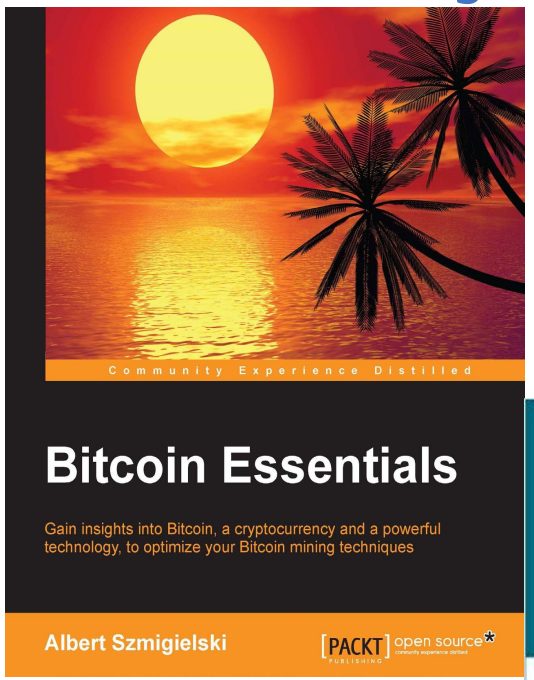


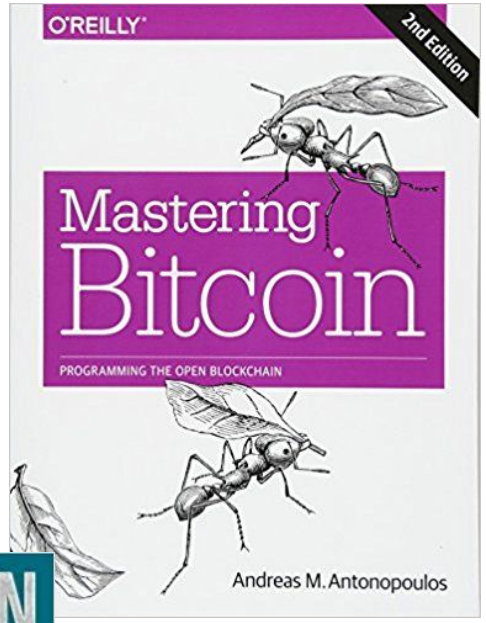
Mineração Profissional

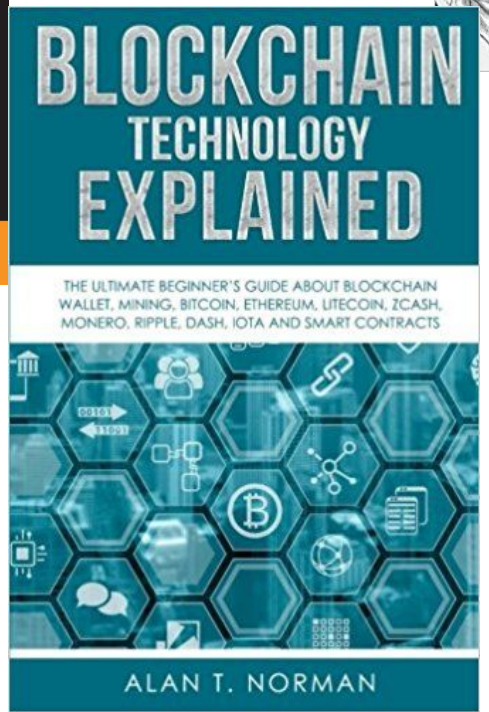
FABC

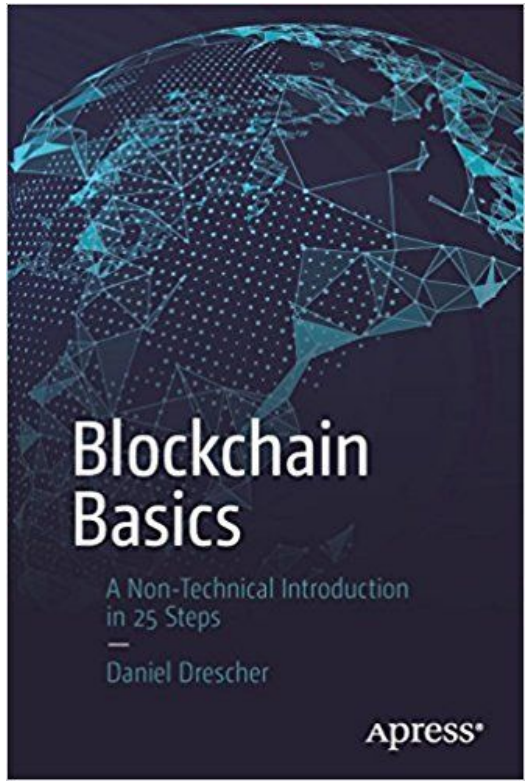
Para abrir os negócios no ramo de mineração

UFABC









Pesquisa

UFABC

- Novas arquiteturas de hardware para mineração
  - Não apenas de BitCoins!
  - Talvez fazer algum trabalho útil com o resultado do PoW
- Avaliação de protocolos de consenso alternativos
  - Proof-of-stake
  - Proof-of-space
- Aplicações da tecnologia de BlockChain em
  - Saúde
  - Governo
  - Sistema bancário