



Criptomoeda e Blockchain

Introdução à Tecnologia

 TÉCNICO
LISBOA

Seminário

2019

Nuno Santos



Criptomoeda e Bitcoin

- ▶ **Criptomoeda:** dinheiro virtual ou digital que assume a forma de tokens (fichas/passes) ou “moedas”
- ▶ **Bitcoin:** A primeira e mais popular criptomoeda
 - ▶ Criada em 2008 por uma pessoa (ou grupo) de nome Satoshi Nakamoto



▶ 2 Criptomoeda e Blockchain - Nuno Santos 2019

Bitcoin: A criptomoeda da Dark Web

Surface Web
Deep Web
Dark Web

▶ 3 Criptomoeda e Blockchain - Nuno Santos 2019

Bitcoin no mercado negro das botnets

- ▶ There's a global market around botnets
- ▶ Who pays:
 - ▶ Internet Advertising companies for downloading adware onto vulnerable PCs
 - ▶ Companies who send spam, viruses and other malware
 - ▶ ...

Bot-herder Owner and Operator

Online Black Market

Click fraud

Identity theft

Spam runs

Phishing attacks

DDoS attack on Web server

BOTNET
Thousands of compromised computers

Spammer

Phisher

Attacker

Malware Protection Center

Spam and host Malware to lure more nodes

▶ 4 Criptomoeda e Blockchain - Nuno Santos 2019



Bitcoin no pagamento de ransomware



Payment will be raised on 5/15/2017 15:58:08
Time Left: 02:23:58:59

Your files will be lost on 5/19/2017 15:58:08
Time Left: 06:23:58:59

About bitcoin
How to buy bitcoins?
Contact Us

Send \$300 worth of bitcoin to this address:
116p7UMMngoj1pMvkpHjcRdfJNXj6LrLn
[Copy](#)

Check Payment Decrypt

▶ 5 Criptomoeda e Blockchain - Nuno Santos 2019



Ransomware: um grande problema

Ransomware Thugs Extort Indiana County for Over \$130,000 in Bitcoin

By Mark Emens — 13/07/2019 05:56 - Updated on 13/07/2019 07:50 In Bitcoin Crime, Cryptocurrency News, News 3 min read

<https://www.ccn.com/news/ransomware-thugs-indiana-county-130000-bitcoin/2019/07/13/>

Trump Blasts Bitcoin For Illicit Use As NY College Is Hit With \$2M Ransomware



<https://www.newsbtc.com/2019/07/12/trump-blasts-bitcoin-for-illicit-use-as-ny-college-is-hit-with-2m-ransomware/>

 Donald J. Trump 
@realDonaldTrump

I am not a fan of Bitcoin and other Cryptocurrencies, which are not money, and whose value is highly volatile and based on thin air. Unregulated Crypto Assets can facilitate unlawful behavior, including drug trade and other illegal activity...

64.8K 1:15 AM · Jul 12, 2019

37.2K people are talking about this

▶ 6 Criptomoeda e Blockchain - Nuno Santos 2019

 **Bitcoins usadas não só por cibercriminosos**

13 Major Retailers and Services That Accept Bitcoin

Shop using several Bitcoin online sites and services

[Share](#) [Pin](#) [Email](#) [PRINT](#)

<https://www.lifewire.com/big-sites-that-accept-bitcoin-payments-3485965>

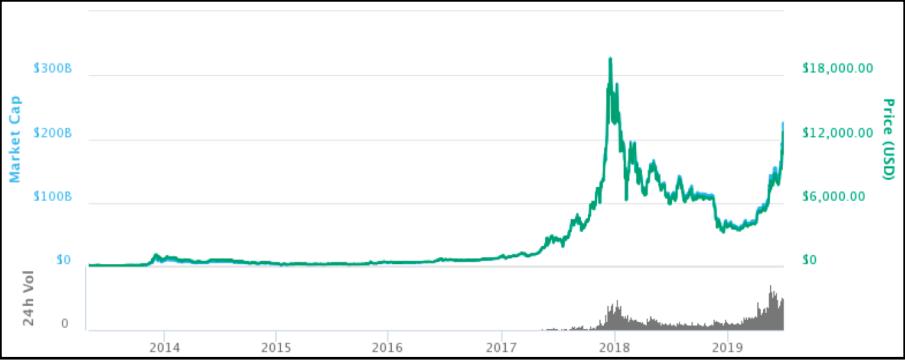
 **Who Accepts Bitcoin as Payment?**

<https://99bitcoins.com/bitcoin/who-accepts/>

Wikipedia	KFC	ExpressVPN
Microsoft	Playboy	Benfica
Expedia	Subway	AT&T
Overstock	Amazon (não directamente)	...

▶ 7 Criptomoeda e Blockchain - Nuno Santos 2019

 **Evolução do preço e volume de Bitcoin**



https://en.bitcoinwiki.org/wiki/Bitcoin_history

Preço da Bitcoin (BTC) entre 2009 e 2019

I BTC = 3,587,520.69 Angolan Kwanza = 9,187.77 Euro = 10,370.70 United States Dollar
(14 Julho 2019)

▶ 8 Criptomoeda e Blockchain - Nuno Santos 2019

 Além da Bitcoin, existem muito mais criptocoins



Litecoin Dash Ripple Monero Bitcoin Cash

The 10 Most Important Cryptocurrencies Other Than Bitcoin (Junho 2019)

<https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/>

- ▶ Litecoin (LTC)
- ▶ Ethereum (ETH)
- ▶ Zcash (ZEC)
- ▶ Dash (DASH)
- ▶ Ripple (XRP)
- ▶ Monero (XMR)
- ▶ Bitcoin Cash (BCH)
- ▶ NEO (NEO)
- ▶ Cardano (ADA)
- ▶ EOS (EOS)

▶ 9 Criptomoeda e Blockchain - Nuno Santos 2019

 Observatórios de criptomoeda online



CRYPTOCURRENCY CHART

#	Name	Price	Price chart (14d)	Change	Supply	Trade volume	Market capitalization	My coins	My value
1	Bitcoin (BTC)	\$10,466.03		-8.27%	17,816,137	\$2,000,155,139	\$186,464,276,508	0	\$0.00
2	Ethereum (ETH)	\$236.92		-11.41%	106,887,708	\$535,926,337	\$25,323,884,513	0	\$0.00
3	Ripple (XRP)	\$0.30		-8.82%	42,566,596,173	\$167,844,234	\$13,073,409,162	0	\$0.00
4	Bitcoin Cash (BCH)	\$309.04		-10.56%	17,888,950	\$111,736,066	\$5,960,806,515	0	\$0.00
5	Litecoin (LTC)	\$89.45		-12.33%	62,676,796	\$175,037,770	\$5,606,869,359	0	\$0.00
6	EOS (EOS)	\$4.37		-7.40%	1,019,800,895	\$118,611,898	\$4,465,374,082	0	\$0.00
7	Binance Coin (BNB)	\$28.90		-7.85%	141,175,490	\$112,576,595	\$4,250,525,529	0	\$0.00
8	Tether (USDT)	\$1.00		+0.20%	3,886,999,504	\$1,227,371,247	\$3,883,501,204	0	\$0.00
9	Bitcoin SV (BSV)	\$134.22		-15.26%	17,854,986	\$49,012,234	\$2,395,484,447	0	\$0.00
10	Cardano (ADA)	\$0.06		-10.78%	25,927,070,538	\$18,739,729	\$2,214,764,205	0	\$0.00

<https://www.cryptocurrencychart.com/>
(Julho 2019)

▶ 10 Criptomoeda e Blockchain - Nuno Santos 2019



Porque é que o Bitcoin é popular no cibercrime?

- ▶ **Sem necessidade de intermediário de confiança**

- ▶ As transacções são feitas à margem da banca

- ▶ **Transacções são privadas**

- ▶ Baseadas em pseudónimos (a pessoa é anónima)

▶ 11

Criptomoeda e Blockchain - Nuno Santos

2019



Pagamentos com Bitcoin

12

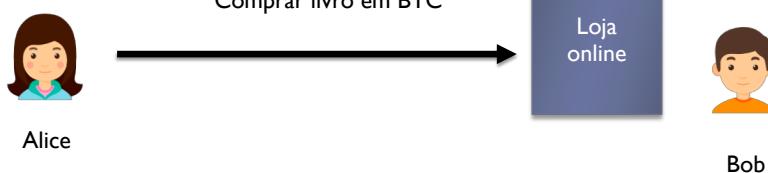
Criptomoeda e Blockchain - Nuno Santos

2019



Cenário de utilização

- ▶ Bob tem uma loja online para venda de livros
- ▶ Alice quer comprar um livro em bitcoin



▶ 13

Criptomoeda e Blockchain - Nuno Santos

2019



Contas, endereços, e carteiras Bitcoin

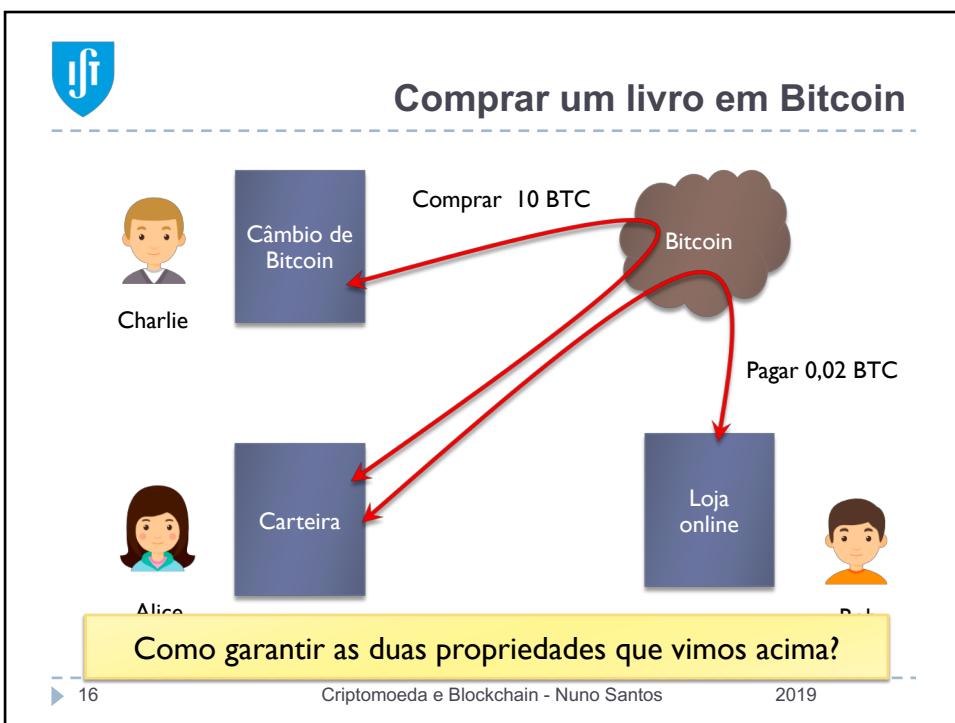
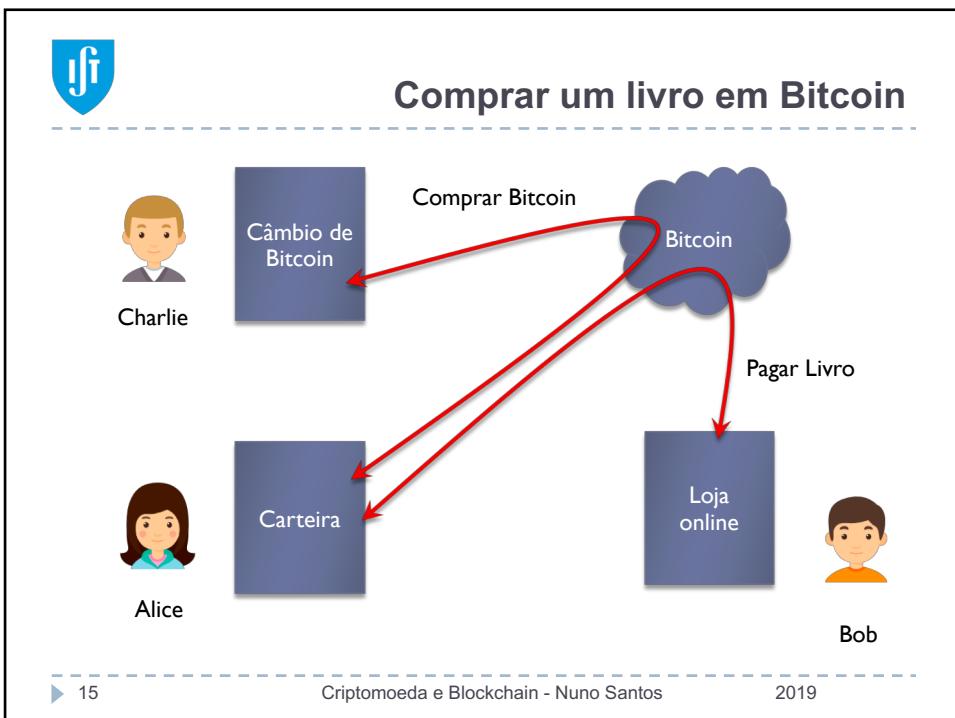
- ▶ Utilizadores precisam de uma **conta** no sistema Bitcoin
- ▶ Cada conta tem um **endereço**
- ▶ Instalam software para gerir o saldo: **carteira / wallet**
 - ▶ App móvel
 - ▶ No serviço web



▶ 14

Criptomoeda e Blockchain - Nuno Santos

2019



Garantir privacidade das transacções

17

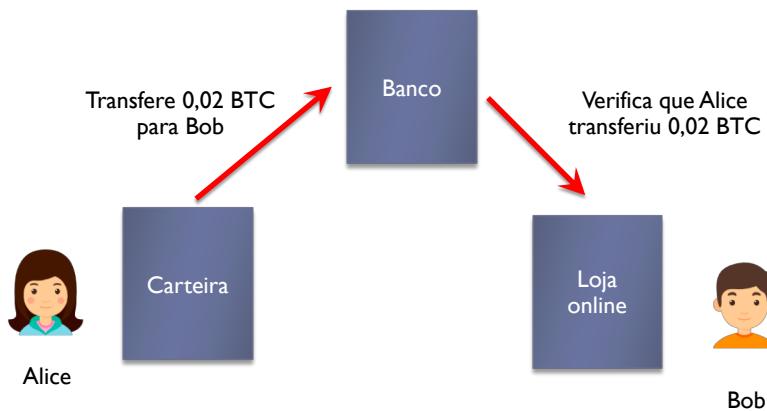
Criptomoeda e Blockchain - Nuno Santos

2019



No sistema bancário tradicional

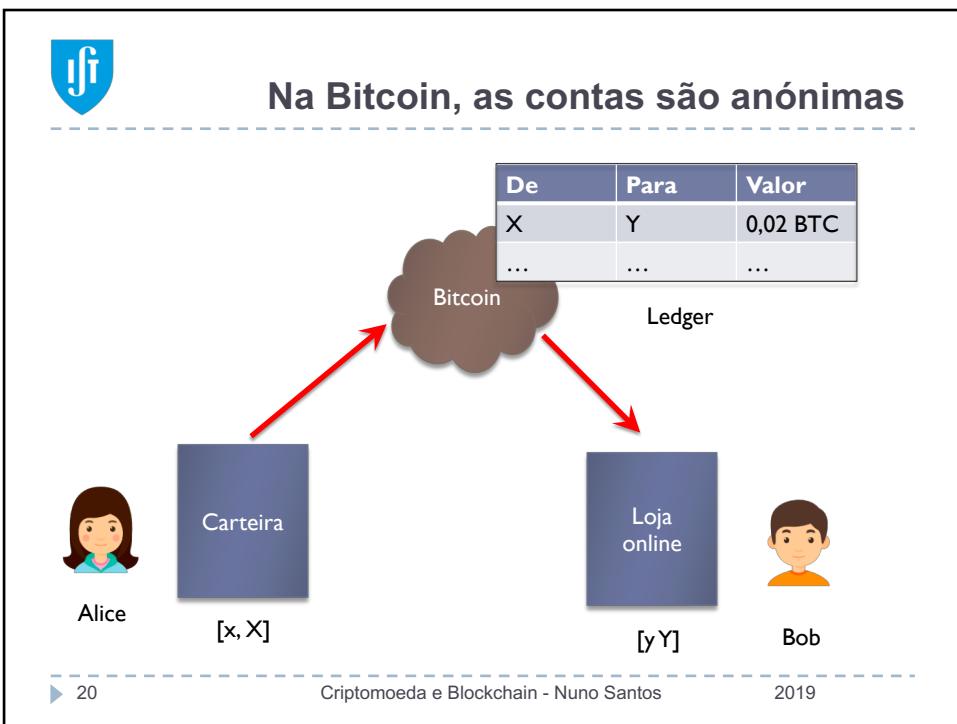
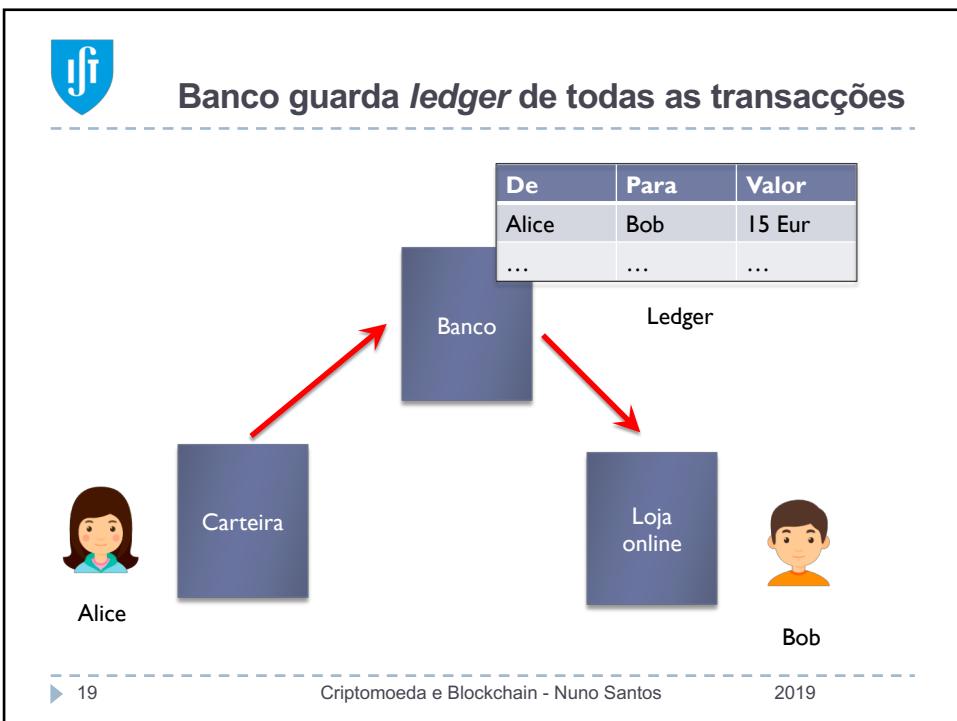
- ▶ O banco mantém contas para todos os utilizadores
 - ▶ Conta: Nome, morada, etc.



▶ 18

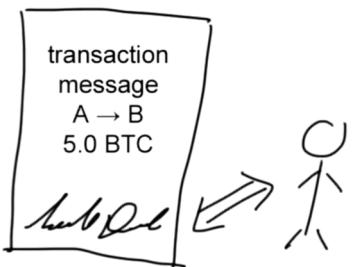
Criptomoeda e Blockchain - Nuno Santos

2019





Transacções em Bitcoin



Digital Signature

30450220078df7c48ed152bd40eae
e4a73afefc3b1ab40fe8ebf422c50c
6262a4c501dad022100f38b330b45
cf233b5b6ea15b36f46a3f1a030635
d52e870c1a15f9c8b469594701 04
...

- ▶ Cada conta tem um endereço que está associada a um par de chaves assimétricas para assinar transacções
- ▶ As chaves públicas são utilizadas para identificar os endereços das contas

Transaction Messages

Digital Signature	
Alice → Bob	5.0 BTC
Alice → Dave	12 BTC
Alice → Juan	2000 BTC
Alice → Bob	14 BTC
	04323784...
	88432738...
	00328434...
	19382637...

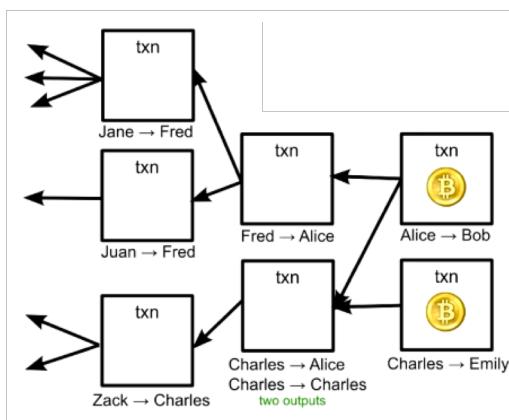
▶ 21

Criptomoeda e Blockchain - Nuno Santos

2019



O ledger é estruturado como grafo de transacções



▶ 22

Criptomoeda e Blockchain - Nuno Santos

2019

O ledger é público para que todos possam verificar

Inputs	Previous output (index) ²	Amount ²	From address ²
	eb38f77560ca..._1	8	1P9SguzjFWgWVAnZBFwimNPV7loma1pgfI
	b9129946c58..._1	0.03	1G8Mk65wVIE5kCVHFSInUTU6st4yVFKM5F
	583794946c85..._15	1	1G9hfnM7ufAPEECdawg5gvUTBB2PxvLr2
	f:9d1cd1c2ac..._1	130	1LqQVnUSMggqjhQBGZwkoobdXJGm9YWyc7
	7b6f7d4a521e..._1	0.55357267	16Kh6XppHUbjgnYQDpRyx9jNE9Aa5Xccb
	544097a30e09..._0	0.03270607	1muDx1gfc757z8AnIUemj46YQgCTw54QN
		139.6	

Outputs	Index ²	Redeemed at input ²	Amount ²	To address ²
	0	1banca27d158...	0.01071174	1F7BgsQbyWTWzEMUKNzzLdkbjnQT9K96m
	1	1bb973b4ccc8...	139.605567	1NT2zFMa11NiCZydh4kcpXRZPf3S6ZPGZ
		139.6		

As chaves públicas são públicas, para se poder verificar as assinaturas

Mas as identidades das pessoas são totalmente desconhecidas

▶ 23 Criptomoeda e Blockchain - Nuno Santos 2019





Importância do intermediário

- ▶ Segurança das transacções e do ledger
- ▶ Credibilidade do valor da moeda
 - ▶ Geração de moeda é controlada
 - ▶ Valor da moeda tem uma relação com um bem real

Solução no sistema Bitcoin: distribuição e blockchain

▶ 25

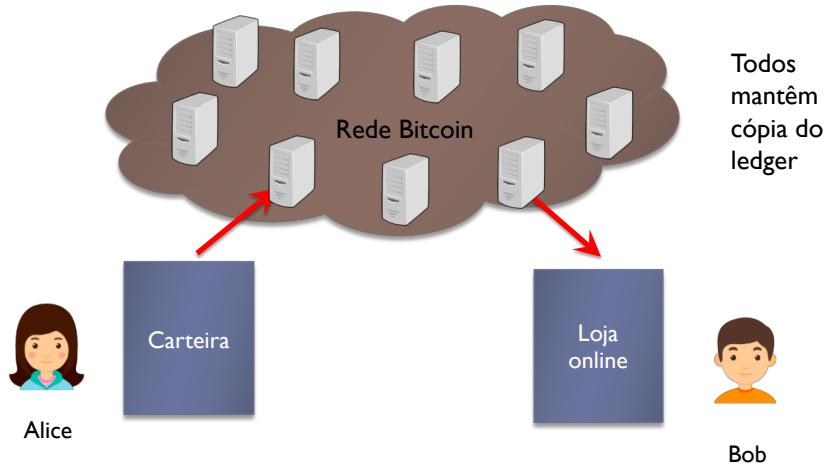
Criptomoeda e Blockchain - Nuno Santos

2019



Como evitar depender num único mediador?

- ▶ O sistema Bitcoin consiste numa rede global de servidores independentes



▶ 26

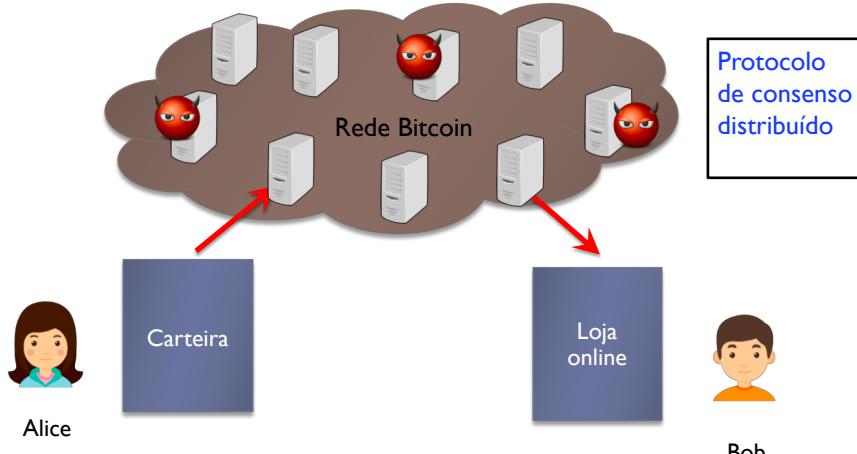
Criptomoeda e Blockchain - Nuno Santos

2019



Como evitar depender num único mediador?

- ▶ Basta que 50% dos servidores bitcoin sejam honestos



▶ 27

Criptomoeda e Blockchain - Nuno Santos

2019



E como garantir a segurança do ledger?

- ▶ Ou seja, que o ledger não é alterado e é actualizado correctamente para cada transacção?
- ▶ Que um utilizador não gasta o mesmo dinheiro mais do que uma vez?
- ▶ Que não incremento mais dinheiro na minha conta?
- ▶ Que não apague transacções passadas?
- ▶ E que o ledger é igual em toda a rede de servidores?

▶ 28

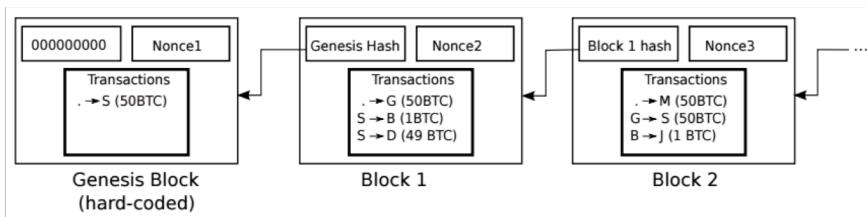
Criptomoeda e Blockchain - Nuno Santos

2019



Blockchain

- ▶ As transacções são guardadas numa estrutura de dados chamada **blockchain**
 - ▶ Não é possível alterar os blocos do passado



▶ 29

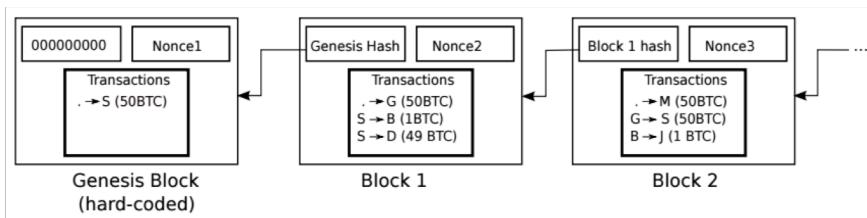
Criptomoeda e Blockchain - Nuno Santos

2019



Blockchain

- ▶ As transacções são guardadas numa estrutura de dados chamada **blockchain**
 - ▶ Não é possível alterar os blocos do passado



Como controlar a geração de moeda e de valor?

▶ 30

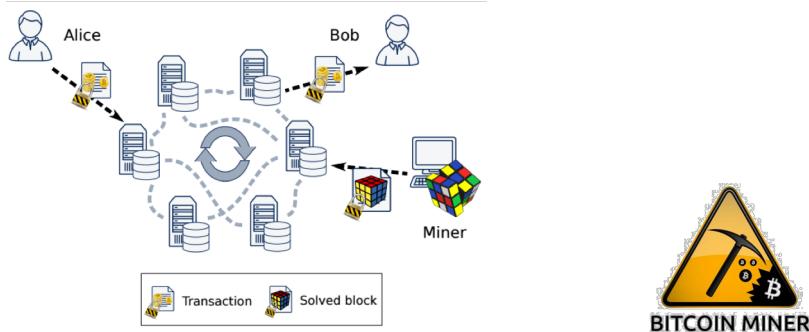
Criptomoeda e Blockchain - Nuno Santos

2019



Mineradores

- ▶ **Mineração** é o processo pelo qual novas bitcoins são adicionadas ao sistema, isto é, criadas
- ▶ **Mineradores** contribuem com computação em troca por oportunidade de serem premiados com uma bitcoin



▶ 31

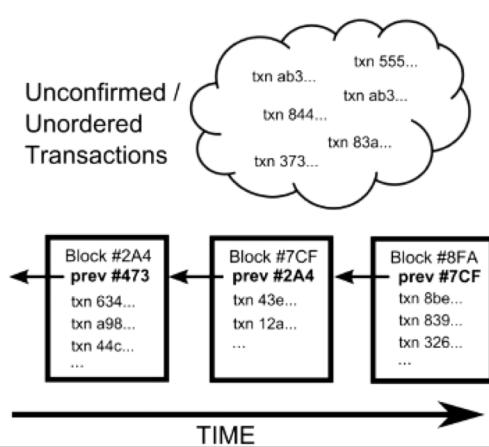
Criptomoeda e Blockchain - Nuno Santos

2019



Os mineradores constroem a blockchain

- ▶ As transacções submetidas não são imediatamente aceites
- ▶ Os mineradores obtém transacções não confirmadas
- ▶ Criam blocos e enviam esses blocos para toda a rede
- ▶ Mas só será eleito um bloco válido para encabeçar a block chain



▶ 32

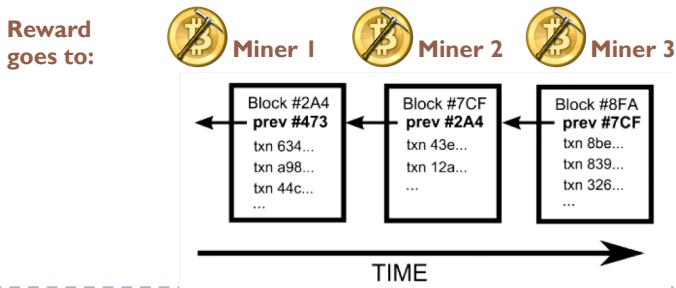
Criptomoeda e Blockchain - Nuno Santos

2019



Controlo de valor através de *proof-of-work*

- ▶ Gerar um bloco implica resolver um desafio matemático muito difícil baseado num algoritmo de hash
 - ▶ Mineradores competem para resolver o problema e obtém recompensa quem o resolver primeiro
 - ▶ A solução para o problema (**Proof-of-Work**) é incluída no bloco e serve como prova de que o minerador resolveu o problema



▶ 33

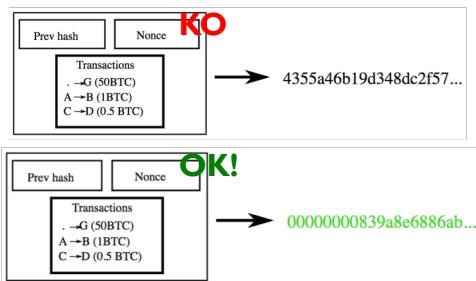
Criptomoeda e Blockchain - Nuno Santos

2019



Exemplo de geração de um bloco

- ▶ **Proof of work:** Encontrar um nonce e calcular a hash de todo o block até ter resultado com 32 zeros no início



- ▶ Se solução encontrada, broadcast para toda a rede
 - ▶ A cadeia mais longa é a considerada válida
 - ▶ Double spending é evitado porque só uma cadeia é válida

▶ 34

Criptomoeda e Blockchain - Nuno Santos

2019

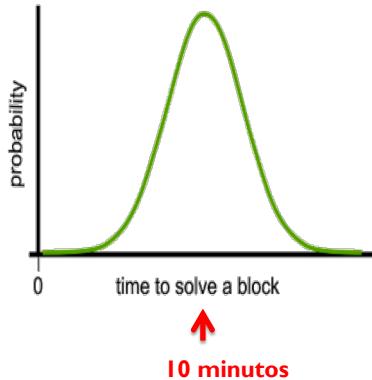


Algoritmo de geração de blocos está calibrado

- ▶ Taxa de geração de blocos em toda a rede: 1 block / 10 min

- ▶ Com cada computador em toda a rede Bitcoin todos tentando adivinhar números para os nonces, demora cerca de ~10 min em média para um minerador encontrar uma solução

Probability Distribution of Block Solving Time



▶ 35

Criptomoeda e Blockchain - Nuno Santos

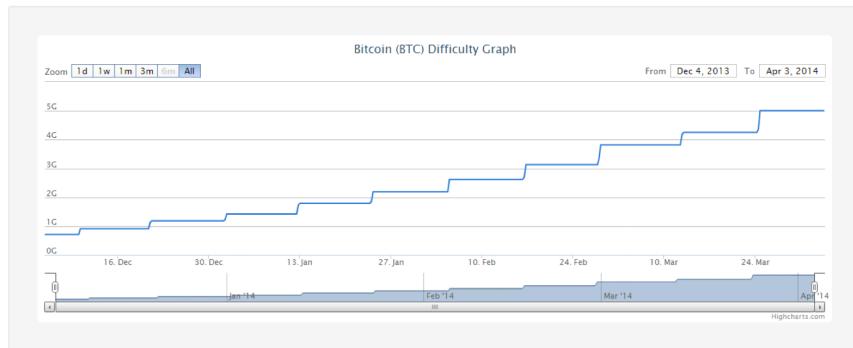
2019



Dificuldade da equação Bitcoin

- ▶ O grau de dificuldade da equação determina a taxa de geração de bitcoins

Bitcoin Difficulty Graph and Bitcoin Difficulty Chart History



▶ 36

Criptomoeda e Blockchain - Nuno Santos

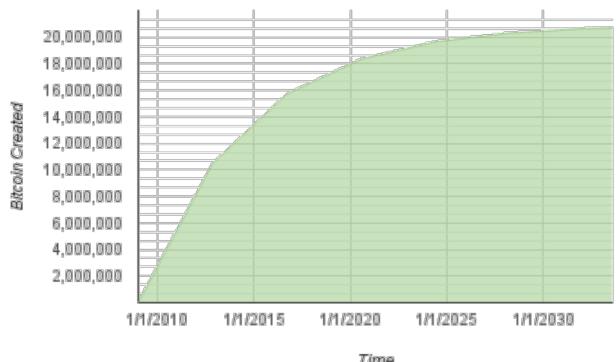
2019



Economia da Bitcoin e criação de moeda

- ▶ Cada bloco, criado a cada 10 min, contém novas bitcoins, criadas do nada
 - ▶ A recompensa de emissão inicial era 50 bitcoin / block, e baixa ½ cada 4 anos
 - ▶ A taxa de geração decresce até 21M bitcoins serem geradas (até 2140)

Bitcoin Money Supply



▶ 37

Criptomoeda e Blockchain - Nuno Santos

2019



Hardware para mineração de Bitcoin



What is Botnet Mining?



BY SHOBHIT SETH | Updated Jun 25, 2019

Cryptocurrency mining botnets are making millions for their creators by secretly infecting various devices across the globe.

<https://www.investopedia.com/tech/what-botnet-mining/>

▶ 38

Criptomoeda e Blockchain - Nuno Santos

2019



Porque é que o Bitcoin é popular no cibercrime?

- ▶ **Sem necessidade de intermediário de confiança**

- ▶ As transacções são feitas à margem da banca

- ▶ **Transacções são privadas**

- ▶ Baseadas em pseudónimos (a pessoa é anónima)

▶ 39

Criptomoeda e Blockchain - Nuno Santos

2019



TÉCNICO
LISBOA

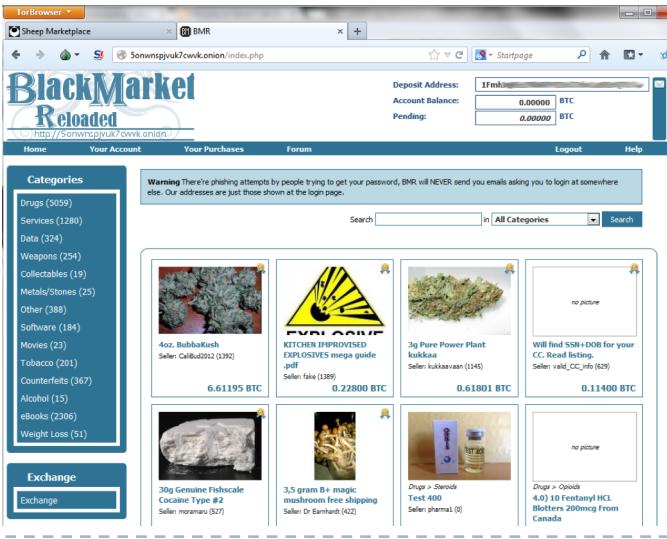
Investigação de transacções Bitcoin

40

Criptomoeda e Blockchain - Nuno Santos

2019

 **Muitos utilizadores Bitcoin prezam o anonimato**



Warning There're phishing attempts by people trying to get your password, BMR will NEVER send you emails asking you to login at somewhere else. Our addresses are just those shown at the login page.

Search All Categories

Categories

- Drugs (5059)
- Services (1280)
- Data (324)
- Weapons (254)
- Collectables (19)
- Metals/Stones (25)
- Other (388)
- Software (104)
- Movies (23)
- Tobacco (201)
- Counterfeits (367)
- Alcohol (15)
- eBooks (206)
- Weight Loss (51)

Exchange

41 Criptomoeda e Blockchain - Nuno Santos 2019

 **Como o Bitcoin ajuda a manter anonimato**

- ▶ Endereços Bitcoin não são mapeados para a identidade real dos utilizadores
- ▶ Transacções Bitcoin não contém informação de teor pessoal
- ▶ Endereços IP dos clientes não é incluído em novas transacções
- ▶ Um utilizador pode gerar tantos endereços Bitcoin quanto queira

42 Criptomoeda e Blockchain - Nuno Santos 2019



Exemplo de geração de várias contas

- ▶ Cada donativo na WikiLeaks vai para nova conta (nova chave pública)
- ▶ Bitcoin permite criar novos pseudónimos



WikiLeaks

Bitcoin is a secure and anonymous digital currency. Bitcoins cannot be easily tracked back to you, and are safer and faster alternative to other donation methods. You can send BTC to the following address:

1HB5XMLmzFVj8ALj6mfBsbifRoD4miY36v

Various sites offer a service to exchange other currency to/from Bitcoins. There are also services allowing trades of goods for Bitcoins. Bitcoins are not subject to central regulations and are still gaining value. To learn more about Bitcoins, visit the website (<https://bitcoin.org>) or read more on [Wikipedia](#).



For a more private transaction, you can click on the refresh button above to generate a new address

▶ 43

Criptomoeda e Blockchain - Nuno Santos

2019



Riscos à quebra de anonimato no Bitcoin

- ▶ Os mecanismos de autenticação em Bitcoin service providers podem relacionar IPs com endereços Bitcoin
- ▶ A cadeia de transacções é transparente e rastreável
- ▶ Endereços Bitcoin expostos na Internet reveal todas as transacções relacionadas com o seu portador
- ▶ Recolher dinheiro de várias contas diferentes pode expôr que os respectivos endereços pertencem ao mesmo utilizador

▶ 44

Criptomoeda e Blockchain - Nuno Santos

2019

As transacções estão relacionadas entre si

É possível determinar como flui o dinheiro, olhando para as várias assinaturas

Inputs ²				
Previous output (index) ²	Amount ²	From address ²	Type ²	ScriptSig ²
eb3877560ca..._1	8	1P95gqzJWgWVAuZlBFwimNPV7LusaplTj	Address	30450220078d7c18ed152fd40eae4a73afe031 044760639da2c0d61584e1a+dab332fec4bb0 + [REDACTED]
b9129936ca5..._1	0.03	18Mk65nV1E5kCvHFShuUTU6nHzVFKM5F5	Address	30450220048776c5ca3733e165052e64c4788dd 04769846c5c5d412784e024c86248c4642d7ck + [REDACTED]
583794946c5..._14	1	1G-H6MDwqAPEECdm-p4gnUTBB2PwLr2	Address	3044022020742364a80048667**2108f14696 0466d415b376e8f33f1563458cfbabb7922d1b4a + [REDACTED]
6941cd1c2ac..._1	130	11pQ1v3MmpqghQBGZtzbobt2Qm0tYWy5...	Address	3046022100ad51188989a4e5e2ea38387503 04bab1a1a5385d4ff0e7683497ab5245669 + [REDACTED]
7b67d3a521c..._1	0.5535726	16Kb6NppH13jgmaYQDpRxx9jNE9A+5Nch	Address	3045022100eeb76e61ab62d386462eadd1d11 044641d1e266fe705038871a31b8fb53d12796 + [REDACTED]
544097a30e09..._0	0.03270607	1JmD1Lqfc757sAnU/mj46YQqCTu54QN	Address	30450221008f9d2cc41493e66849ccce10615 04de2576f490b0d16188bebd06ca7b148166a4b + [REDACTED]

Outputs ²				
Index ²	Redeemed at input ²	Amount ²	To address ²	Type ²
0	1baaca27d148...	0.01071174	1F7BgrQbvWTWfEMUKNzrLdkbjnQT9K96m	Address
1	1b6973b4ccc8...	139.605567	1NT2fEMa11NgCZhkqgNPZPf3S6ZPG2	Address

▶ 45 Criptomoeda e Blockchain - Nuno Santos 2019

Heurística shared-spending

- ▶ **Shared spending:** indício de controlo de diferentes contas pelo mesmo utilizador
 - ▶ Dois inputs da mesma transação são provavelmente do mesmo utilizador

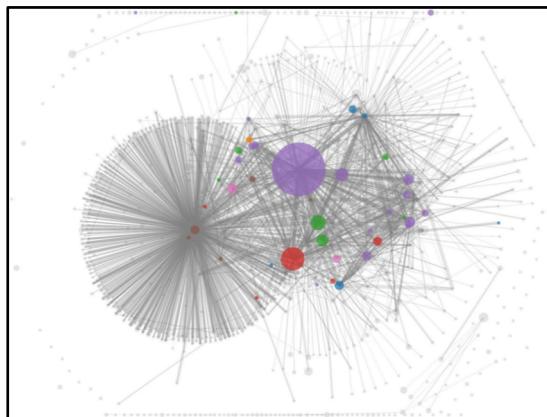
To pay for the teapot, Alice has to create a single transaction having inputs that are at two different address. In doing so, Alice reveals that these two addresses are controlled by a single entity.

▶ 46 Criptomoeda e Blockchain - Nuno Santos 2019



Clustering de endereços

- Em 2013, investigadores usaram heurísticas para observar padrões de transacções



The sizes of these circles represent the quantity of money flowing into those clusters, and each edge represents a transaction.

47

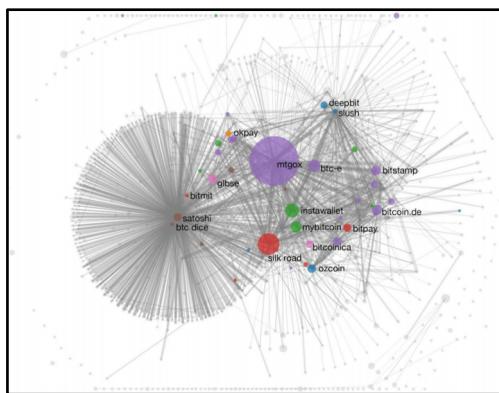
Criptomoeda e Blockchain - Nuno Santos

2019



Associar identidades reais aos clusters

- Etiquetar por transacção:** para aferir a identidade associada aos endereços, efectuar transacção com esse service provider, ex., depositar bitcoins, comprar um item, etc.
- O endereço do servide provider será conhecido e a tx aparecerá na blockchain



By transacting with various Bitcoin service providers, researchers were able to attach real world identities to their clusters.

48

Criptomoeda e Blockchain - Nuno Santos

2019



Identificar indivíduos nos clusters

1. Transacção directa

- ▶ Revela pelo menos um endereço pertencente àquele indivíduo

2. Descuido

- ▶ Por vezes as pessoas revelam endereços Bitcoin em forums públicos

3. Evolução dos algoritmos de desanonimização

- ▶ Geralmente melhoraram ao longo do tempo à medida que mais dados se tornam acessíveis publicamente

▶ 49

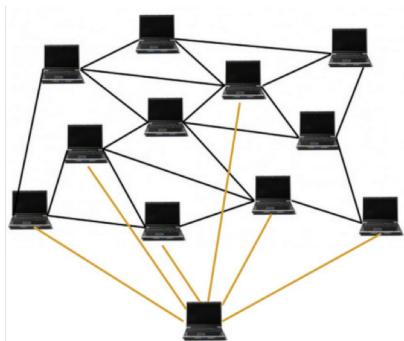
Criptomoeda e Blockchain - Nuno Santos

2019



Análise do protocolo e rede Bitcoin

- ▶ Para interagir com a rede Bitcoin, é necessário enviar mensagens para toda a rede a partir de várias máquinas
- ▶ Vários nós podem colaborar para determinar a proveniência das mensagens



▶ Bitcoin protocol sniffer

- ▶ As mensagens não são cifradas; tentar relacionar Bitcoin address – IP address

▶ Sybil attack

- ▶ Tentar infiltrar vários nós na rede controlados pelo investigador e interceptar mensagens dos clientes

▶ 50

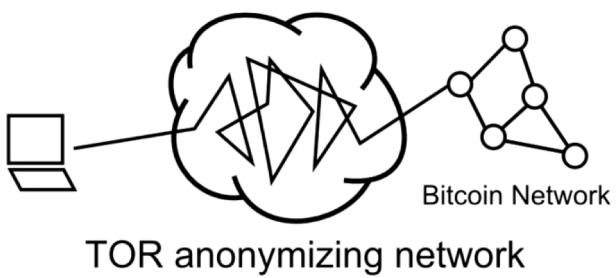
Criptomoeda e Blockchain - Nuno Santos

2019



Bitcoin + Tor

- ▶ Uma abordagem para aumentar anonimato



▶ 51

Criptomoeda e Blockchain - Nuno Santos

2019



Conclusões

- ▶ Bitcoin é um sistema de criptomoeda revolucionário que permite a realização de pagamentos online anónimos e totalmente descentralizados
- ▶ A principal tecnologia que está por detrás da segurança e robustez do sistema bitcoin é a blockchain e o seu sistema de mineração baseado em proof-of-work
- ▶ Apesar das garantias de anonimato do sistema Bitcoin serem muito elevadas, os investigadores têm explorado várias abordagens para identificar a identidade de utilizadores através da inspecção do ledger público Bitcoin

▶ 52

Criptomoeda e Blockchain - Nuno Santos

2019