Blockchain

André Sá de Mello - 8531911
Andreas Munte Foerster - 7143997
Rafael Gallo - 8531758
Guilherme Muzzi da Rocha - 8626274
Weslei Renato de Lima - 6511258

Sumário

- Histórico
- Tecnologia
  - Conceitos
  - *Blockchain*
- Aplicações
- Cases

Histórico - Bitcoin

Bitcoins: moedas digitais baseadas em criptografia que podem ser enviadas e recebidas pela Internet.

- Em 1990 o criptógrafo norte-americano David Chaum trata em seu artigo intitulado “Untraceable Electronic Cash” os principais pontos de falha presentes em sistemas de pagamento tradicionais como cartões de crédito.
- Em 1998 Wei Dai apresenta uma proposta teórica intitulada “b-Money” contendo protocolos para criar e manter dinheiro digital descentralizado.
- Em 2002 o criptógrafo Hal Finney propõe um método de reutilização de tokens digitais para serem utilizados como dinheiro chamado “Reusable Proofs of Work” (RPOW).
- Em 2005 Nick Szabo apresenta a descrição do sistema “BitGold” contendo arranjos econômicos, porém, sem implementação.
- No dia 31 de Outubro de 2008 Satoshi Nakamoto publica o artigo intitulado “Bitcoin: a Peer-to-Peer Electronic Cash” onde apresenta o projeto do sistema Bitcoin e inicia o desenvolvimento do mesmo.

2009

- 3 de Janeiro: Criação do primeiro bloco de Bitcoin (chamado: “genesis block”). Foram gerados 50 BTC. Hora: 18: 15: 05 (de Greenwich).
- 9 de Janeiro: Sai a primeira versão Bitcoin v0.1
- 12 de Janeiro: Primeira transação Bitcoin (bloco 170). Remetente: Satoshi Nakamoto. Destinatário: Hal Finney.
- 5 de Outubro: Foi publicado o primeiro câmbio de Bitcoin em relação ao dólar na Bolsa: $1 = 1,309.03 BTC. Negociações lançadas na Bolsa de New Liberty Standard.
- 16 de Dezembro: Sai a versão Bitcoin v0.2

2010

- 22 de Maio: Primeira compra feita online. Compra de uma pizza por 10 mil moedas (que no momento equivaliam a 25 dólares).
- 11 de Junho: Anúncio da versão Bitcoin v0.3

2011

- 28 de Janeiro: Foi gerado o bloco 105000 (até o momento já haviam sido emitidos 5,25 milhões de Bitcoins).
- 31 de Março: Foi aberta a primeira bolsa para troca de Bitcoins por Reais do Brasil (BitcoinBrazil).

2012

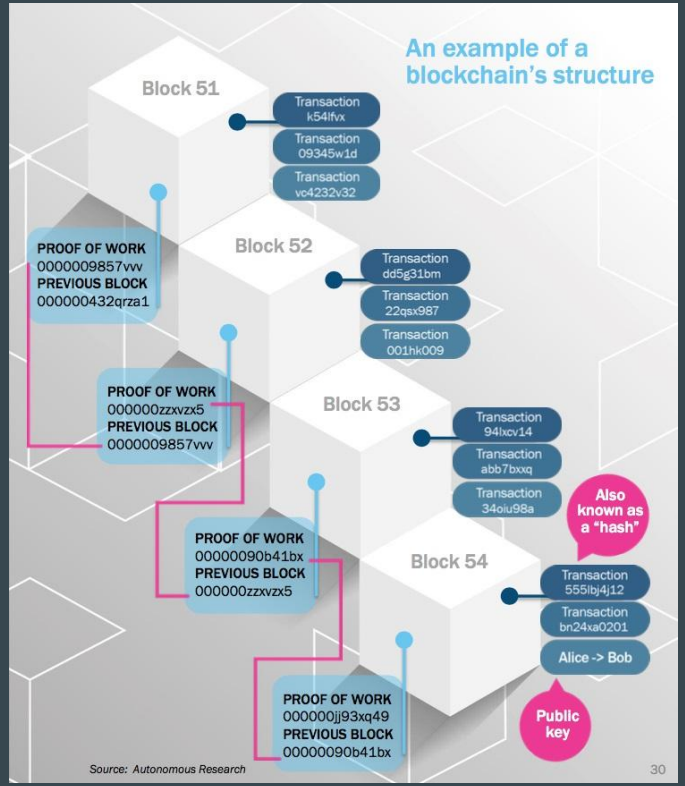
- 15 - 16 de Setembro: Ocorrência da primeira conferência de Bitcoin em Londres.

2013

- 19 de Fevereiro: Concluída a oitava versão de cliente Bitcoin.

Tecnologia - Conceitos

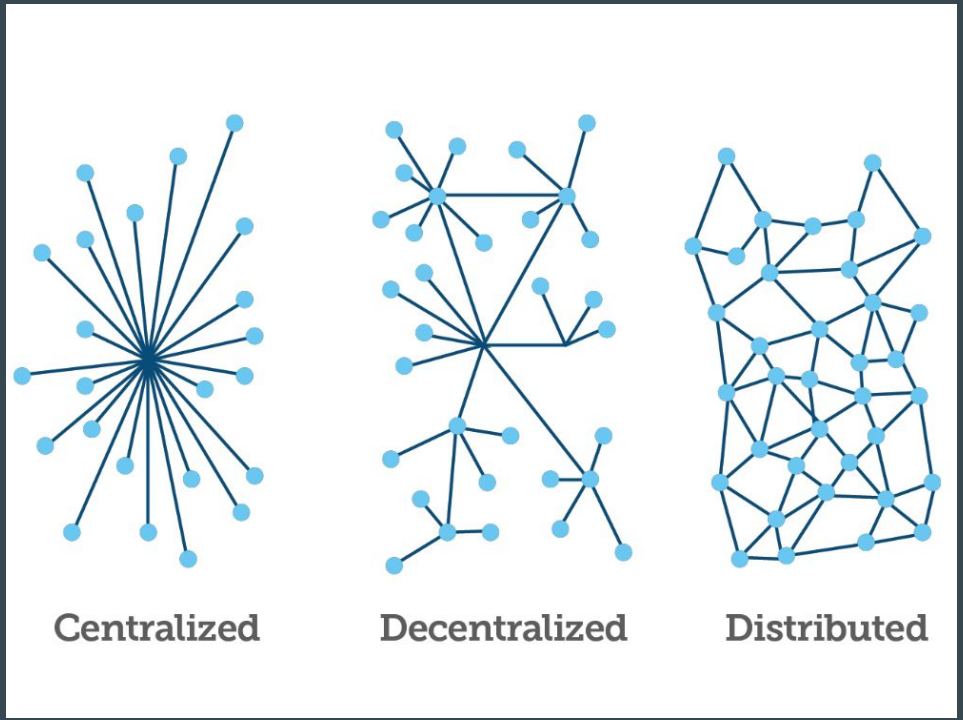
- O que é *Blockchain*?
  - Um banco de dados autônomo, progressivo, que mantém uma lista de registros ou transações.
  - Cada bloco contém uma lista de registros, e cada bloco é encadeado com o anterior.
    - Literalmente uma cadeia de blocos.



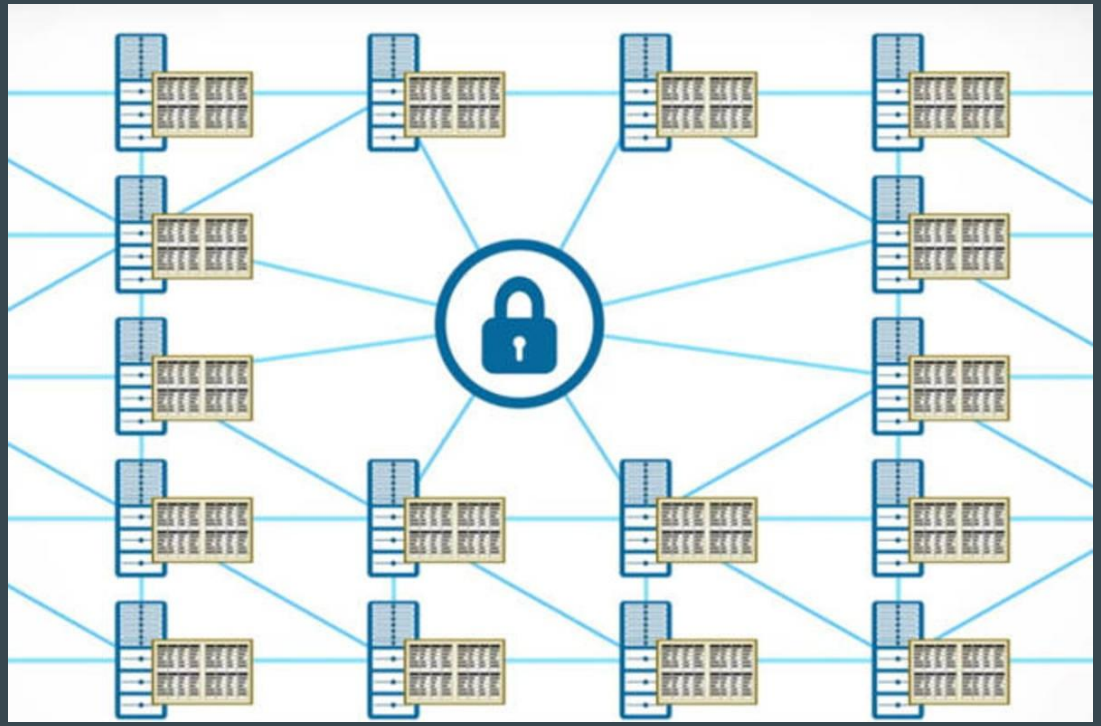
Tecnologia

- **Distribuído**

Não há uma entidade central que aprova as transações e estabelece normas.



Tecnologia



- **Público**

As cadeias são replicadas na rede, e qualquer um pode ler os registros validados por cada bloco.

- **Seguro**

Os registros são validados por consenso global, e são irreversíveis e imutáveis.

Tecnologia

- **Confiável**

A natureza distribuída requer consenso dos servidores, permitindo transações entre entidades desconhecidas.

- **Automático**

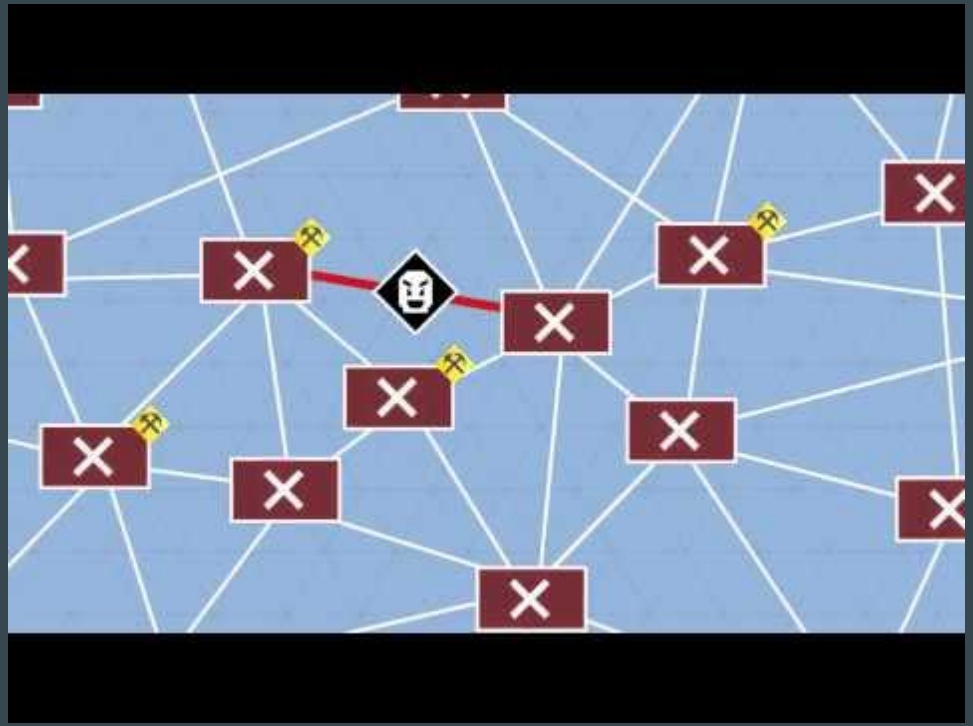
Software impede transações duplicadas ou conflitantes.

Tecnologia

Smart Contracts

Permite programar o comportamento da transação. Quando é efetivada uma transação, o contrato é automaticamente executado.

Deu origem ao chamado Blockchain 2.0.



https://youtu.be/oSP-taqLWPQ

Tecnologia - Conceitos

- *Distributed Autonomous Corporations* (DAC)
  - Generalização do Bitcoin: moeda representa créditos que podem ser trocados por serviços:
    - Troca de posses (BitShares)
    - Serviços de nome de domínio (DomainShares)
    - Contribuições para pesquisa (Gridcoin)
    - Troca de caronas (La`Zooz)
  - Contribuição para o serviço é proporcional à recompensa.
  - Infraestrutura é baseada na tecnologia Blockchain.

Tecnologia

- **Métodos de formação de consenso**
  - O Bitcoin usa **Proof of Work (POW)** para validar as transações.
  - **Desvantagem**: lento, e trabalho realizado é inútil.
  - Alternativas foram desenvolvidas:
    - **Proof Of Stake (POS)**
    - **Delegated Proof Of Stake (DPOS)**

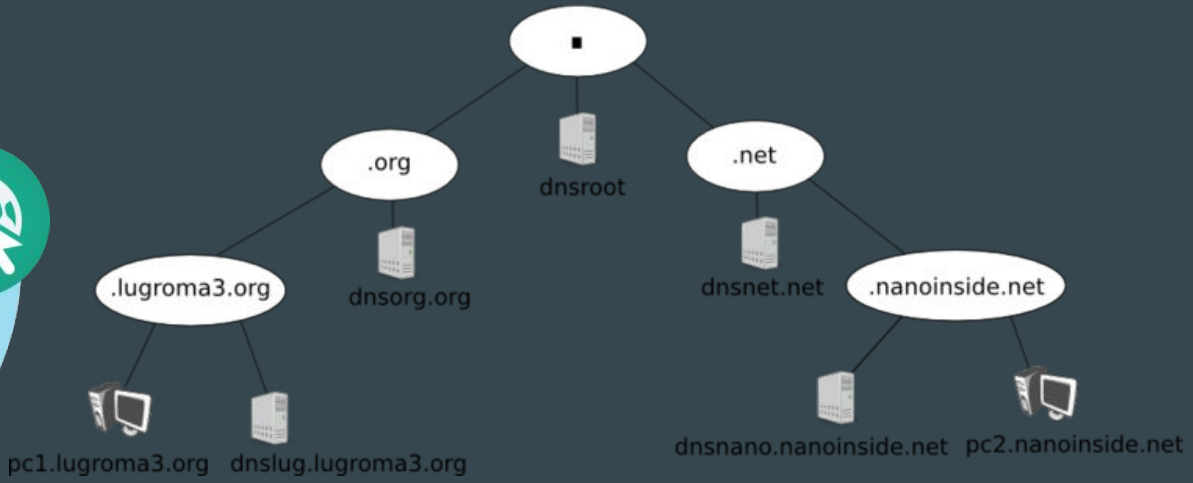
Tecnologia

- **Blockchain 2.0**
  - Permite **misturar** vários tipos de registro (transações, mensagens, etc.).
  - Permite **intercâmbio** nativo com outros tipos de moeda (inclusive as tradicionais) e posses.
  - Sistema POW é **lento**, então criptomoedas desse tipo **não são práticas**.
- **Blockchain 3.0**
  - Uso de DPOS permite validar **grande número de Transações Por Segundo**
    - Desenvolvedores do BitShare alegam alcançar 100 000 TPS.
    - Isso é equiparável ou superior a sistemas financeiros em atuação!

Aplicações

Certificado digital

DNS



Aplicações

- **Comércio global anônimo**
  - Proteção da privacidade
  - Permite contornar restrições governamentais*
- **Compilações de fatos públicos**
  - Enciclopédias
  - Jornalismo

Aplicações

- **Sistemas bancários centralizados**
  - É possível usar moedas tradicionais
  - Não permite duplicações
  - Transparência
- **Computação distribuída**
  - Pesquisa científica (*Gridcoin*, *Primecoin*, etc.)
  - Supercomputadores (*Zennet*)

Aplicações

Validação de:

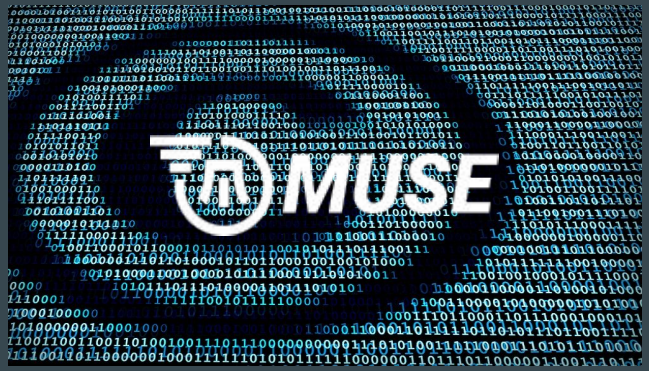
- Votos
- Registros públicos
- Pagamento de impostos
- Testamentos
- **Contratos** (*Ethereum*)
- Comprovantes
- Certificados
- Certidões
- Títulos
- Ações (*BitShares*)
- Registros médicos
- Serviços computacionais

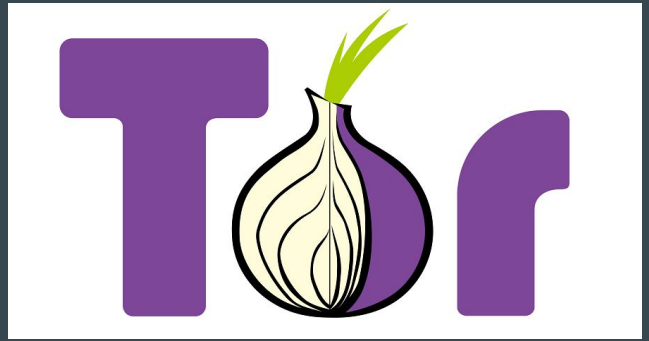
Aplicações

Aplicação	Implementação	Concorrente
Comércio decentralizado	OpenBazaar	Craigslist
Serviços de caronas decentralizado	La`Zooz	Uber
Redes sociais	Twister, Gems	Twitter, Facebook
Mensagens instantâneas	Bitmessage	WhatsApp
Arquivos em nuvem	Storj	Dropbox
Validação de identidade	Onename, BitID, Bithandle	VeriSign

Aplicações

- Rastreamento de **direitos autorais**:
  - Ideia antiga, desde a incepção do Projeto Xanadu.
  - MUSE implementa (para músicas).
- Inteligências artificiais "**seguras**".
- Validação de doação de banda para sustentar redes voluntárias como **TOR.**





Blockchain Applications by Sector (selected)

Economics and Markets	Government & Legal	IOT	Health	Science, Art, AI
• Currency • Payments & Remittance • Banking & Finance • Clearing & Settlement • Insurance • FinTech • Trading & Derivatives • QA & Internal Audit • Crowdfunding	• Transnational orgs • Personalized governance services • Voting, propositions • P2P bonds • Tele-attorney services • IP registration and exchange • Tax receipts • Notary service and document registry	• Agricultural & drone sensor networks • Smarthome networks • Integrated smartcity, connected car, smarthome sensors • Self-driving car • Personalized robots, robotic companions • Personalized drones • Digital assistants	• Universal EMR • Health databanks • QS Data Commons • Big health data stream analytics • Digital health wallet • Smart property • HealthToken • Personal development contracts	• Community supercomputing • Crowd analysis • P2P resourcenets • Film, dataviz • AI: blockchain advocates, friendly AI, blockchain learners, digital mindfile services
Crucial Blockchain Properties				
• Cryptoledger • Decentralized network • Trustless counterparties • Independent consensus-confirmed transactions	• Permanent record • Public records repository • Notarization time-stamping hashes • Universal format • Accessibility	• Communication (messaging) • Large-scale coordination • Entity ingress/egress • Transaction security	• Universal format • Large-scale multi-data-stream integration • Privacy and security • Real-time accessibility	• Large-scale infrastructural element for coordination • Checks-and-balances system for 'good-player' access

http://www.amazon.com/Bitcoin-Blueprint-New-World-Currency/dp/1491920491

Banks & financial services players exploring blockchain opportunities

Case 1 - Bancos

- Bitcoin cresce cada vez mais no mercado
- Mas é a tecnologia por trás que chama atenção dos bancos
- Blockchain
  - Validação rápida de transações
  - Menor custo com infraestrutura
- Mais de 25 bancos, liderados pelo FinTech (Tecnologia Financeira) desenvolve aplicação de blockchain para o mercado

Case 1 - Bancos

- Banco da Inglaterra
  - Sistema RSCoin
  - Pesquisadores da University College London
  - Objetivos
    - Emissão de moeda digital
    - Pagamento mais eficiente
    - Sistema financeiro mais resistente

Case 1 - Bancos

- Banco da Inglaterra
  - Realizar muitas transações, grandes ou pequenas, de forma rápida e dispendiosa
  - Criptografia - resistente a falsificação
  - Documento digital para validação
  - Organização de terceiros para realizar transações
  - Contabilidade Central
    - Muitas transações, ambiente mais familiar, controle

Case 1 - Bancos

- Banco da Inglaterra
  - Transações parcialmente ou totalmente anônimas
  - Testada com 30 computadores diferentes (nuvem da Amazon)
  - Artigo do RSCoin - Simpósio em San Diego

Case 1 - Bancos

- Goldman Sachs
  - Bitcoin como um ato de abertura
  - Blockchain toma o cenário do palco
  - Elimina a necessidade de um intermediário
    - Acelera processos manuais

Case 1 - Bancos

- Goldman Sachs
  - Aplicações segundo o Banco
    - Sistemas de votação
    - Registros de Veículos
    - Taxas Bancárias
    - Acordos comerciais

Case 1 - Bancos

- UBS
  - Banco mais aberto
  - Equipe dedicada (Crypto 2.0 - Londres)
  - Mais de 20 casos de uso
  - Moeda Virtual (Bondcoin)
    - Vinculada a moeda real
    - Permite transação direta entre as partes

Case 1 - Bancos

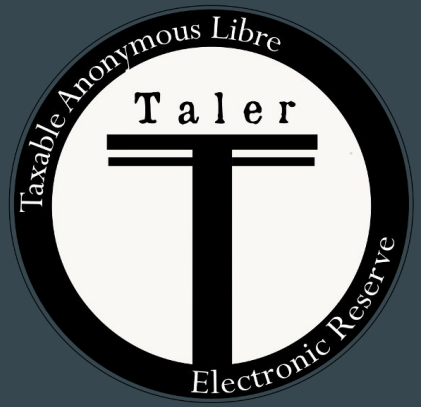
- UBS
  - Experimentos
    - Contratos Inteligentes
      - Recriar emissão de título
      - Cálculo de juros
      - Pagamentos
    - Trata diretamente fluxo de informações e dinheiro

Case 2 - Governo

- Idéia:
  - Automatizar validações de documentos governamentais com blockchains.
- Problemas:
  - Rede Bitcoin depende de mineradores anônimos para validar transações.
  - A privacidade e semi-anonimato do Bitcoin não são desejadas para um uso governamental.

Case 2 - Governo

- Soluções - Blockchains Privadas:
  - GNU Taler.
    - É um software livre (Free Software Fondation).
    - Sistema de pagamentos eletrônicos.
    - Está ainda em desenvolvimento.
    - Será focada na garantia de que o governo pode identificar os cidadãos e manter um registro de suas rendas e, portanto, garantir pagamentos de impostos.



Case 2 - Governo

- Soluções - Blockchains Privadas:
  - GreenCoinX:
    - Tem como alvo justamente os governos.
    - É flexivel e modificável para se adaptar às necessidades de cada governo.
    - Está sendo considerada uma das melhores plataformas para governos, por ser simples e transparente.

Case 2 - Governo

- Casos:
  - Estônia: Começou o programa e-Residency no fim de 2015, com alcançe mundial.
  - Ucrânia: Está transferindo a votação para o sistema e-Vox que é baseado no Blockchain Ethereum.
  - Russia: Também pretende implementar Blockchain nas suas votações.
  - Reino Unido: Está começando pesquisas de implementação de Blockchains no governo.

Referências

- https://www.technologyreview.com/s/600980/a-bitcoin-style-currency-for-central-banks/
- http://www.businessinsider.com/what-is-blockchain-2016-3
- http://www.wsj.com/articles/bitcoin-technologys-next-big-test-trillion-dollar-repo-market-1459256400?mod=WSJ_TechWSJD_moreTopStories
- http://fortune.com/2016/03/04/crisis-in-bitcoin-rise-of-blockchain/
- http://www.npr.org/sections/alltechconsidered/2016/05/04/476597296/not-just-bitcoin-why-blockchain-is-a-seductive-technology-to-many-industries
- https://www.technologyreview.com/s/545806/microsoft-bets-that-bitcoin-style-blockchains-will-be-big-business/
- https://bitshares.org/
- https://www.ethereum.org/
- http://www.gridcoin.us/
- http://www.slideshare.net/lablogga/bitcoin-and-blockchain-explained-cryptocitizen-smartnetwork-trust
- https://news.bitcoin.com/future-use-cases-for-blockchain-technology-copyright-registration/

Referências

- https://www.cryptofresh.com/
- https://en.wikipedia.org/wiki/Block_chain_(database)
- https://medium.com/@andysingleton/the-third-generation-of-blockchain-tech-will-mix-and-match-with-real-world-systems-93b6cc3b1eb9#.rtuqvkv3x
- http://www.coindesk.com/russia-national-settlement-depository-blockchain-voting/
- http://cryptorials.io/glossary/delegated-proof-of-stake/
- https://bitshares.org/technology/delegated-proof-of-stake-consensus/

Perguntas?