"Criptomoedas - Vantagens e riscos"

84.º Seminário GEE/GPEARI

27 de junho de 2023

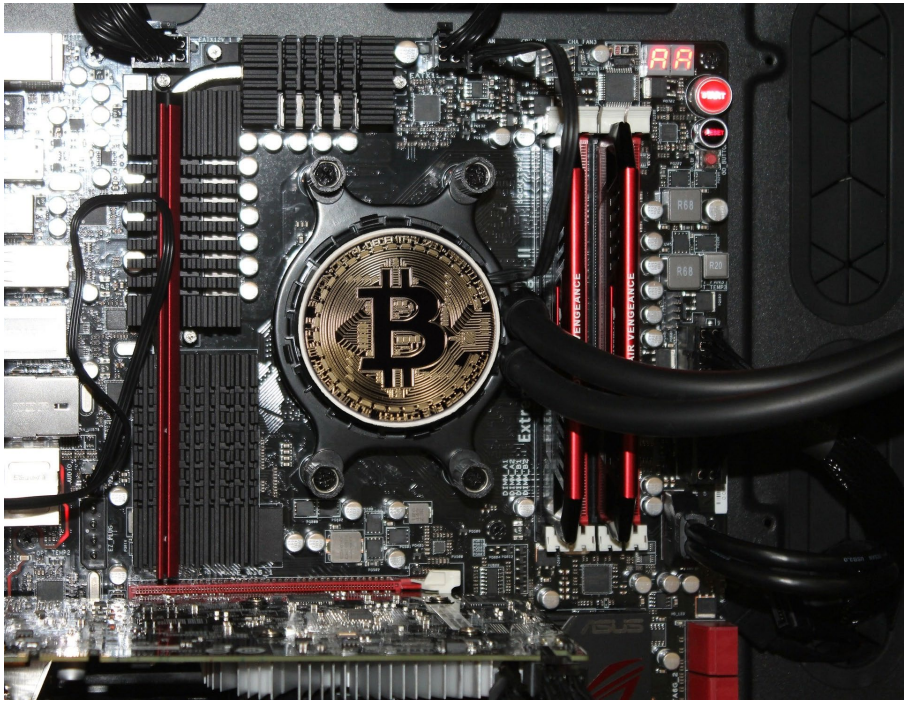
Gabriel Osório de Barros

Diretor de Serviços de Análise Económica no Gabinete de Estratégia e Estudos

Índice

Introdução

- **Evolução histórica: troca de mercadorias → dinheiro → dinheiro digital**
- **Criptomoedas: dinheiro digital baseado em criptografia**
- **Diferenças entre criptomoedas e moeda fiduciária tradicional**
- **Vantagens e riscos das criptomoedas**

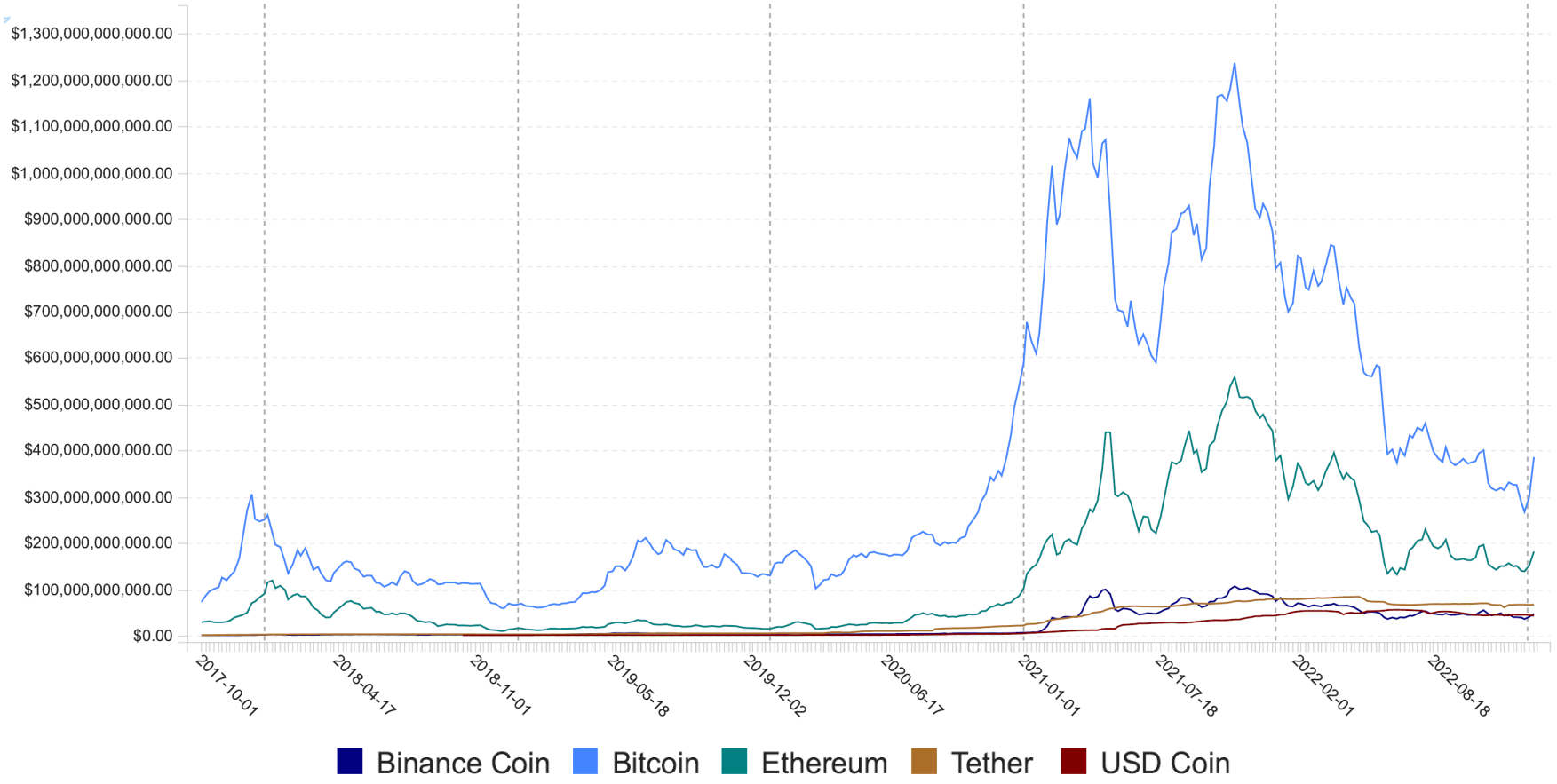


História das Criptomoedas

- Conceitos iniciais de liberalismo e cripto-anarquismo
- Estudos iniciais de Chaum: criação de "dinheiro eletrónico incondicionalmente irrastreável"
- Dwork e Naor (1992): técnica computacional para controlo de acesso a recursos compartilhados
- Proposta de Wei Dai sobre B-Money (1998)
- Satoshi Nakamoto e o *white paper* do Bitcoin (2008): criação de uma moeda descentralizada baseada em criptografia
- Início da Bitcoin network e mineração das primeiras bitcoins (2009)
- Aparição de outras criptomoedas (altcoins) como Ethereum e Cardano
- Flutuação do valor de mercado das principais criptomoedas (2021 - 2023)
- Aumento de plataformas para a comercialização de bitcoins

História das Criptomoedas

Evolução do valor de mercado das 5 principais criptomoedas (em USD), entre 1 de outubro de 2017 e 15 de janeiro de 2023



Fonte: https://www.cryptocurrencychart.com/

Moeda Fiduciária vs Criptomoedas

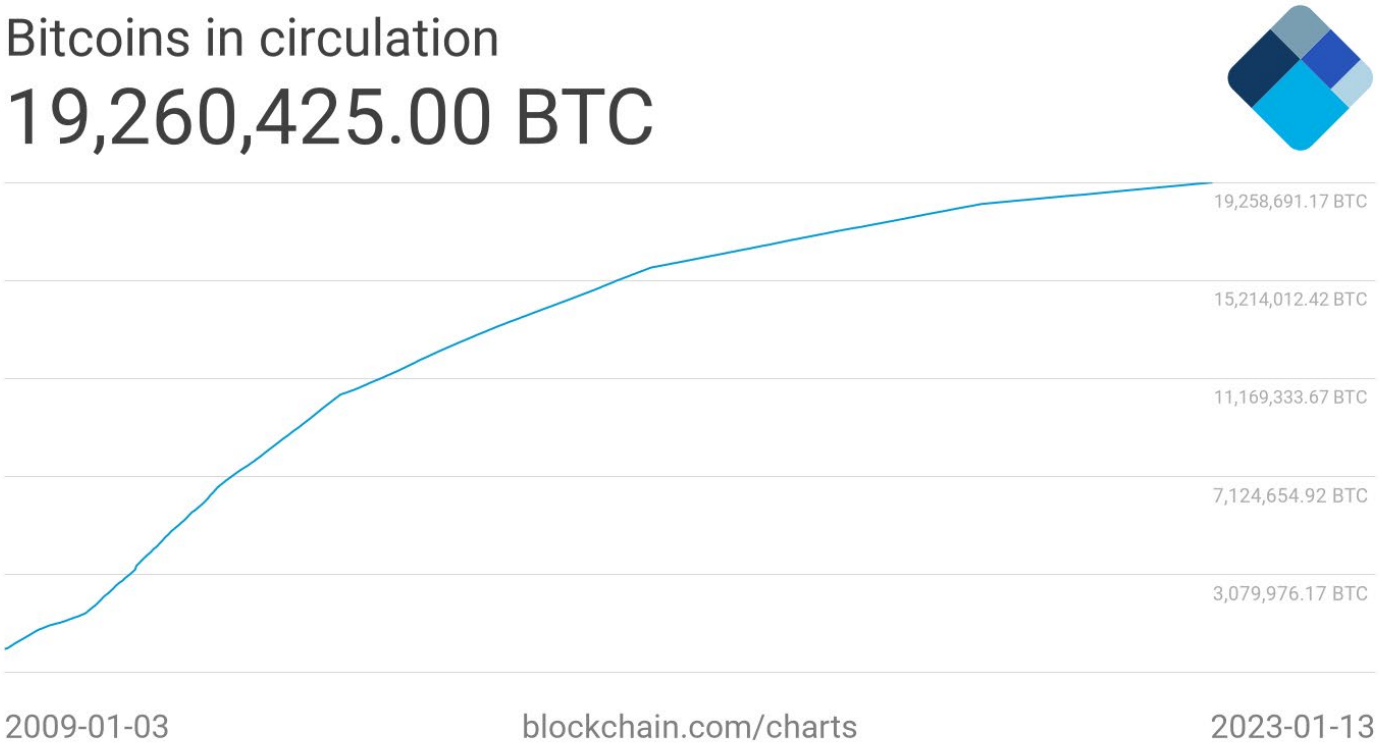
- **Características comuns a moeda fiduciária e criptomoedas: unidade de medida, meio de pagamento, divisibilidade e portabilidade**
- **Criptomoedas são globais**
- **A aceitação de criptomoedas ainda não é generalizada**
- **Instabilidade do valor das criptomoedas**
- **Falta de controle e supervisão de bancos centrais nas criptomoedas**
- **Diferenças-chave entre moeda fiduciária e criptomoedas: mineração vs emissão, controle centralizado vs descentralizado, anonimato, regulamentação e segurança**

A Revolução das Bitcoins

- Bitcoin: a primeira e mais usada criptomoeda
- Aumento significativo na circulação de Bitcoins desde 2009, quase alcançando 19.3 milhões de moedas mineradas
- Flutuação do preço de mercado do Bitcoin ao longo do tempo
- Confidencialidade garantida para os usuários do Bitcoin
- Funções semelhantes às de um banco: acesso exclusivo do proprietário à conta, registro de transações e gerenciamento de contas
- Uso de chaves públicas e privadas para transações
- Implementação do *Unspent Transaction Output* (UTXO) para garantir a exclusividade das transações
- Transações de Bitcoin são armazenadas em blocos, formando uma *blockchain*

A Revolução das Bitcoins

Bitcoins em circulação[1]
(número total de bitcoins "minerados" em circulação na rede)

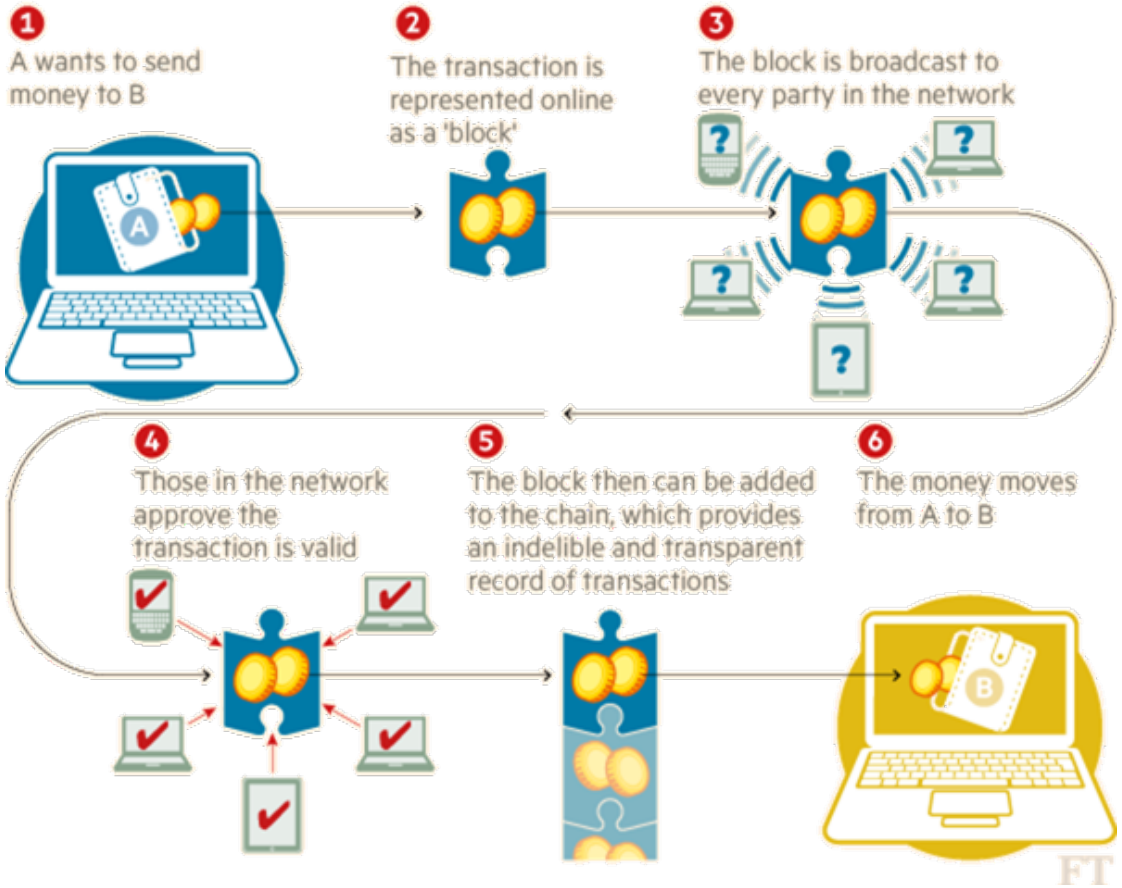


Fonte: https://www.blockchain.com/en/charts/total-bitcoins

[1] Número total de bitcoins que já foram "minerados" (*mined*), ou seja, o fornecimento atual de bitcoins na rede (https://www.blockchain.com/charts/total-bitcoins)

- ***Blockchain***
  - Estrutura de dados fundamental para o registro de transações de criptomoedas
  - Caracterizado pela transparência e independência
  - Previne a falsificação de moedas e a reversão de transações
- **Descentralização**
  - Verificação de consenso através do *proof-of-work*
  - Validação por pares que permite decisão descentralizada
  - Distribuição do *ledger* entre vários nós para garantir a integridade e segurança
- **Anonimato / Pseudonimato**
  - Identidades dos usuários são difíceis de serem obtidas
  - Utilização de chaves públicas e privadas para autenticação
  - Prevenção contra acesso indevido e atividades maliciosas
- **Imutabilidade**
  - Decentralização permite a imutabilidade da informação
  - Uso de *hashes* criptográficos para garantir a imutabilidade
  - Cadeia de custódia transparente e pública para verificação de autenticidade e integridade dos dados

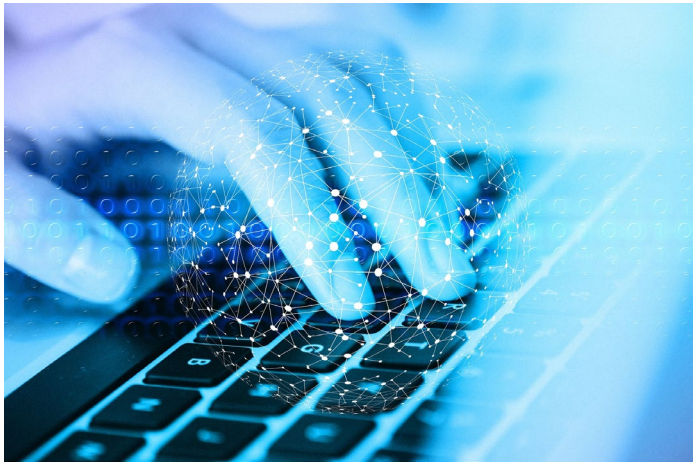
Transação no *Blockchain*



Fonte: Financial Times
(https://assets.weforum.org/wp-content/uploads/2015/12/151103-blockchain-bitcoin-technology-banking-fintech-FT.png)

Externalidades do Blockchain

- **Adaptação a novas aplicações em áreas como energia, indústria, finanças automóvel ou saúde**
- **Possibilita maior segurança e descentralização no armazenamento e transferência de informação**
- **Torna mercados mais "democráticos", deslocando o controlo da informação das empresas para os consumidores**
- **Empresas podem adotar a tecnologia *blockchain* para fortalecer as suas cadeias de valor**
- **Pode permitir aos consumidores evitar a falsificação, provando a identidade do comerciante e do consumidor, monitorizando o movimento dos produtos e criando registros verificáveis**



Utilização prática

- **Facilita a compra e venda de bens e serviços**
- **A aceitação de criptomoedas ainda é limitada, mas está a crescer**
- **Existem vários exemplos de utilização de Criptomoedas em várias áreas, embora não seja de aceitação geral - lojas online, viagens, imobiliário, ou caridade, entre outras**
- **Podem ser usadas para compras online através de vários sites**
- **Alguns estabelecimentos físicos também aceitam criptomoedas embora não seja frequente**
- **As criptomoedas são populares para investimento e *trading***

Volatilidade

- Criptomoedas são conhecidas pela sua volatilidade
- A volatilidade das criptomoedas é mais alta em comparação com outros ativos, como ouro ou o índice S&P 500
- Ganhos elevados são possíveis, mas elevadas perdas também
- O preço das criptomoedas é influenciado por várias choques, alguns dos quais estão relacionados com medidas de governos

Volatilidade no período entre 7 de agosto de 2015 e 15 de janeiro de 2023

	Standard deviation	Volatility
Gold	0,012	18%
S&P 500	0,008	15%
Bitcoin	0,039	74%
Ethereum	0,064	122%

Investimento com Criptomoedas

- Criptomoedas têm permitido arrecadação de fundos para investimento em projetos via ICO
- ICO é uma forma inovadora de obtenção de financiamento, mas vem com riscos significativos
- Investimento vs especulação: a alta volatilidade das criptomoedas torna-as impróprias como reserva de valor
- Risco de esquemas Ponzi: os ganhos dos primeiros investidores são pagos com o capital dos novos investidores
- É aconselhável a diversificação do investimento para reduzir o risco

Ausência de regulação

- As criptomoedas não estão sujeitas a regulamentação, o que traz incertezas jurídicas e risco de fraude
- A falta de regulação retira dos bancos centrais um importante instrumento de política monetária
- A falta de definição clara dos direitos e obrigações das partes envolvidas potencia atividades criminais
- Os riscos para os consumidores incluem alta volatilidade, falta de proteção ao consumidor e falta de transparência na formação de preços
- A utilização de criptomoedas permite uma economia paralela isenta de impostos
- A conversão de dinheiro em criptomoeda também pode ser uma maneira de lavar dinheiro e financiar o terrorismo

Consumo energético e impacto ambiental

- O algoritmo "*proof-of-work*" das criptomoedas consome uma grande quantidade de recursos, incluindo capacidade de computação e energia elétrica
- A Bitcoin, a criptomoeda mais usada, consome mais de 78 TWh por ano, um valor próximo ao consumido pelo Chile.
- A pegada de carbono anual do Bitcoin é de 43,61 Mt de CO_2 por ano.
- A pressão sobre os computadores leva à rápida desvalorização de equipamentos menos eficientes, gerando mais de 40 kt de lixo eletrónico por ano.
- A Bitcoin tem uma alta pegada de lixo eletrónico, chegando a 449 gramas por transação.

Questões de segurança e ataques

- **Acesso ao *Clipboard* através de *Malware*: Atacantes podem explorar falhas de segurança para roubar criptomoedas**
- **Ataque de Gasto Duplo ou Ataque de 51%: Uma entidade maliciosa pode gastar a mesma criptomoeda duas vezes se controlar mais de 50% do poder de processamento**
- **Ataque de Negação de Serviço Distribuído (DDoS): Ataques DDoS visam interromper o tráfego normal de um servidor ou rede inundando o alvo com tráfego excessivo de internet**
- **Ataque Sybil: Inunda a rede com nós de zero potência, criando muitas falsas entidades**
- ***Forking*: Cria diferentes versões da história de transações, podendo ser usado para validar transações anteriormente consideradas inválidas**
- **Mineradores de criptomoedas mal-intencionados: Os atacantes podem usar *malware* para obter acesso aos computadores das vítimas para aumentar o poder de processamento**
- ***Chain hopping*: Os hackers movem fundos entre diferentes redes blockchain para aproveitar diferenças de segurança ou regulatórias**
- **Ataques de *ransomware*: Os hackers criptografam os arquivos de um usuário e exigem pagamento em criptomoeda para restaurar o acesso**

Credibilidade das Criptomoedas

- Início marcado por escândalos: Caso *Silk Road* e Colapso da *Mt. Gox*
- Crescentes preocupações sobre uso de criptomoedas para atividades ilegais
- Questões sobre segurança e estabilidade após o colapso da *Mt. Gox*

- Outros casos destacados: *Bitfinex* (2016) e *Coincheck* (2018)
- Apesar dos desafios, crescimento contínuo e proposta de alternativa viável às moedas tradicionais, 2022 foi um ano crítico, com preços em queda significativa e várias empresas indo à falência
- Falências: *FTX*, *BlockFi*, *Three Arrows Capital*, *Voyager Digital*, *Celsius Network*
- Riscos para os investidores: bancos centrais não asseguram perdas, complexidade e demora no processo de falência

Novas moedas digitais

- Aparecimento de novas formas de criptomoedas: *stablecoins*
- Preocupações dos bancos centrais com impacto das *stablecoins* na estabilidade financeira e política monetária
- Principais *stablecoins*: *Tether*, *USD Coin*, *Binance*
- *Diem* (anteriormente Libra): criptomoeda do Facebook
- Implementação de moedas digitais por bancos centrais: Digital Yuan (China), Digital Euro (UE)
- Prós e contras das moedas digitais: segurança, facilidade de uso, custo, anonimato parcial
- Não-linearidades na criação de moedas digitais por bancos centrais

Comentários finais

- Criptomoedas: visibilidade e adesão significativas, mas não isentas de riscos
- Principais vantagens: facilidade e rapidez de transações, privacidade, disponibilidade 24/7, baixos custos
- Principais riscos: volatilidade elevada, potencialidades para atividades criminosas, ausência de uma autoridade central, dificuldade de identificação dos usuários, falta de sistema de garantia de depósitos
- Poucos comerciantes aceitam criptomoedas, limitando sua utilização
- Potencial do *blockchain* para revolucionar infraestrutura financeira e económica
- Desafios futuros: melhorar a segurança das criptomoedas, criar moedas digitais dos bancos centrais para combater riscos
- As criptomoedas são ainda recentes, o seu futuro é incerto e depende de várias variáveis

Muito obrigado.

Gabriel Osório de Barros (gabriel.barros@gee.gov.pt)

Referências:

- Barros, Gabriel Osório de (2019). "*Cryptocurrencies - Advantages and Risks of Digital Money*". Tema Económico 67. Gabinete de Estratégia e Estudos.
- Barros, Gabriel Osório de (forthcoming). "*Cryptocurrencies - Advantages and Risks of Digital Money*". Blockchain as a Technology For Environmental Sustainability (Capítulo aceite). CRC Press.