# Aula 014 - Altcoins

## Alternative Coins

Prof. Rogério Aparecido Gonçalves[1]
rogerioag@utfpr.edu.br

[1]Universidade Tecnológica Federal do Paraná (UTFPR)
Departamento de Computação (DACOM)
Campo Mourão - Paraná - Brasil

Programa de Pós Graduação em Ciência da Computação
**Mestrado em Ciência da Computação**
PPGCC17 - Tópicos em Redes de Computadores e Cibersegurança

# Agenda i

1. Introdução às Altcoins
2. Theoretical foundations
3. Difficulty adjustment and retargeting algorithms
4. Bitcoin limitations
5. Extended protocols on top of Bitcoin eevelopment of altcoins
6. Development of altcoins
7. Próximas Aulas

# Agenda ii

8. Referências

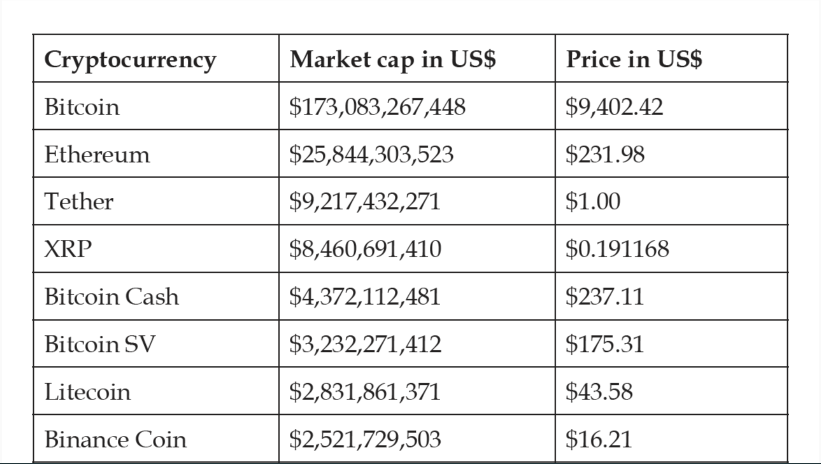
# Introdução às Altcoins

# Objetivos

- Apresentação de uma Visão Geral sobre rede Bitcoin e pagamentos.

# Altcoins

- ‘Altcoins’ is a term used to describe coins other than the original electronic cash bitcoin.



| Cryptocurrency | Market cap in US$ | Price in US$ |
|---|---|---|
| Bitcoin | $173,083,267,448 | $9,402.42 |
| Ethereum | $25,844,303,523 | $231.98 |
| Tether | $9,217,432,271 | $1.00 |
| XRP | $8,460,691,410 | $0.191168 |
| Bitcoin Cash | $4,372,112,481 | $237.11 |
| Bitcoin SV | $3,232,271,412 | $175.31 |
| Litecoin | $2,831,861,371 | $43.58 |
| Binance Coin | $2,521,729,503 | $16.21 |

# Bitcoin power consumption

Bitcoin's Proof of Work (PoW) consensus mechanism has several drawbacks, particularly extremely high energy requirements. This is the main reason why alternatives PoW to were proposed, such as Proof of Stake (PoS).

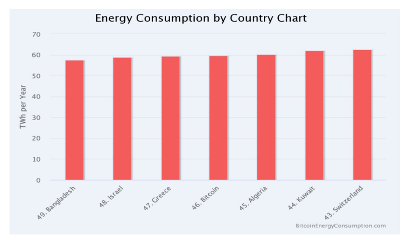


**Figura 2:** Energy consumption by country – Bitcoin at No. 46.

- Revisiting Bitcoin's carbon footprint, (February 2022); how Bitcoin got dirtier after the Chinese mining crackdown in 2021.
- Bitcoin Energy Consumption Index, the Bitcoin Energy Consumption Index provides the latest estimate of the total energy consumption of the Bitcoin network.

# Theoretical foundations

# Difficulty adjustment and retargeting algorithms

# Difficulty adjustment and retargeting algorithms

PoW algorithms use difficulty adjustment and retargeting algorithms, which are simple arithmetic formulas that help adjust the difficulty of solving the PoW problem:

- Bitcoin
  - $T = Timeprevious * timeactual/2016 * 10min$
- Kimoto Gravity Well
  - $KGW = 1 + (0.7084 * pow((double(PastBlocksMass)/double(144)), -1.228))$
- Dark Gravity Wave
  - $2222222/(((Difficulty + 2600)/9)^2)$
- DigiShield
  - $Newdifficulty = (previousdifficulty)xSQRT[(150seconds)/(lastsolvetime)]$
- MIDAS
  - A more complex algorithm for difficulty adjustment.

# Bitcoin limitations

# Limitações do Bitcoin i

- Privacy and anonymity
- To address such issues, various proposals have been made:
    - Mixing protocol
    - Inherent anonymity
    - CoinSwap
    - TumbleBit
    - Dandelion

# Extended protocols on top of Bitcoin eevelopment of altcoins

# Extended protocols on top of Bitcoin i

- **Colored coins:** developed to represent digital assets on the Bitcoin blockchain. Coloring a bitcoin refers to updating it with some metadata representing a digital asset
- **Counterparty:** another service that can be used to create custom tokens that act as a cryptocurrency and can be used for various purposes, such as issuing digital assets on top of the Bitcoin blockchain

# Development of altcoins

# Development of altcoins

The following are some required parameters, or parameters to be tweaked, if forking from another code base: Consensus algorithms Difficulty adjustment algorithms Inter-block time Block rewards Reward halving rate Block size and transaction size Interest rate Coinage Total supply of coins

# Bloco Genesis i

## Bloco Genesis

O Bloco Genesis ou bloco $\#0$ foi *hardcoded* (codificado) por suas características especiais: ele é o único que não aponta para nenhum bloco anterior. No seu *hash* foi encriptado o bloco junto com a mensagem *"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"*, manchete do jornal naquele dia. Além de servir como prova datada, a manchete escolhida representa justamente uma crítica ao sistema bancário.

# Atividade

- Consider what parameters were changed in order to create the Litecoin blockchain from Bitcoin.

# Word Cloud

# Leitura Recomendada

### Leitura Recomendada

**Capítulo 6: Bitcoin Network and Payments**

**Livro**: IMRAN BASHIR. Mastering Blockchain : Distributed Ledger Technology, Decentralization, and Smart Contracts Explained, 2nd Edition.

# Próximas Aulas

# Próximas Aulas

- Pagamentos com *Bitcoin*.

# Referências

# Referências i

Imran, Bashir. 2018. *Mastering Blockchain : Distributed Ledger Technology, Decentralization, and Smart Contracts Explained, 2nd Edition.* Packt Publishing. https://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=1789486&lang=pt-br&site=eds-live&scope=site.