inesc id lisboa
DEFINING TECHNOLOGY

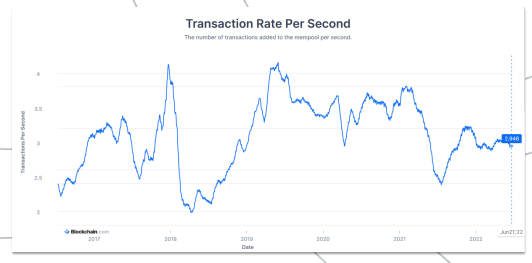
Efficient and sustainable permissionless Proof-of-Space blockchain systems

Advanced Studies Diploma in Computer Science and Engineering

João Martinho (joao.e.martinho@tecnico.ulisboa.pt)

Motivation

https://digiconomist.net/bitcoin-energy-consumption/



https://www.blockchain.com/charts/transactions-per-second

Problem

Sustainability

Security

Performance

Contributions

Sustainability
Proof-of-Useful-Space

- Replace Proof-of-Work
- Use disk space to generate proofs
- Proof generation virtually inexpensive
- Use user-relevant data → no waste
- Nothing-at-stake issue

Security
Random beacons

- Uniform randomness
- Unpredictable and unbiasable
- Non-manipulable intervals
- Nothing-at-stake deterrence:
  - Set the growth rate
  - Single source of randomness

Performance

Throughput (tx/s)

Confirmation time (s)

ADVANCED STUDIES DIPLOMA IN COMPUTER SCIENCE AND ENGINEERING

Prof. Miguel Matos & Prof. João Barreto

29/06/2022

INESC-ID – Instituto de Engenharia de Sistemas e Computadores, Investigação e Desenvolvimento em Lisboa

Rua Alves Redol, 9 1000-029 Lisboa Portugal Tel. +351.213100300 Email: info@inesc-id.pt

This work was supported by national funds through FCT, Fundação para a Ciência e a Tecnologia, under projects UIDB/50021/2020 and Ainur (PTDC/CCI-COM/4485/2021),