



André Gouveia
Analista financeiro

“As criptomoedas são demasiado voláteis como investimento”

19 de janeiro de 2021

O nosso especialista em criptomoedas, André Gouveia, entrevistou Miguel Pupo Correia, professor no Instituto Superior Técnico e autor de diversos projetos na área da cibersegurança.



Miguel Pupo Correia é o representante nacional na European Blockchain Partnership, que está a desenvolver uma blockchain única no mundo: a a European Blockchain Services Infrastructure.

Miguel Pupo Correia, formado em Engenharia Eletrotécnica e de Computadores, é professor associado com agregação do Instituto Superior Técnico da Universidade de Lisboa e investigador sénior do INESC-ID. Esteve envolvido em vários projetos de investigação no âmbito da cibersegurança, mas confessa que quando a [Bitcoin](#) apareceu não lhe prestou muita atenção.

Alguns anos mais tarde, decidiu investigar as [criptomoedas](#), ao perceber que a blockchain se assemelhava ao tema do seu doutoramento sobre segurança e ataques indesejáveis nos computadores.

André Gouveia: *Enquanto especialista em blockchain, como vê o fenómeno das criptomoedas? É um adepto?*

Miguel Correia: Sob o ponto de vista tecnológico, acho as criptomoedas muito interessantes. Por um lado, parece-me uma aplicação da confiança distribuída, que faz

todo o sentido. Por outro, surpreendeu-me. As aplicações que investigávamos durante os anos 2000 eram muito diferentes: armazenamento de ficheiros, bases de dados, gestão de nomes, etc.

Ainda mais interessante do que as criptomoedas parecem-me os tokens ou assets virtuais. A ideia de virtualizar e transacionar tokens, que representam diferentes tipos de objetos e valores, parece-me ter imenso potencial. Apesar disso, não me considero um adepto das criptomoedas para utilização na prática. Nesta fase, parecem-me uma forma problemática de pagamento e são demasiado voláteis como investimento. Em Portugal, temos alternativas muito mais simples, como MBWay, MBnet, etc.

André Gouveia: *A segurança do mecanismo de consenso é vital. O proof- of-work é um sistema já muito testado e implementado com sucesso. Os algoritmos proof-of-stake serão igualmente seguros?*

Miguel Correia: Uma coisa que aprendi em 20 anos de investigação em cibersegurança é que os adversários (hackers, ou como lhes quiser chamar) são inventivos. No caso de sistemas como estes, que movem grandes quantias, a motivação para os manipular pode ser grande. No entanto, os algoritmos proof-of-stake parecem-me tão seguros como os proof-of-work.

No início de dezembro, foi lançada a rede Ethereum 2.0, que usa proof-of-stake. Em algumas horas, já havia mais de 20 mil validadores, que, para terem esse papel, tinham de depositar 32 Eth, ou seja, cerca de 18 mil euros cada. Isto mostra bem que existe uma grande comunidade que confia no proof-of-stake: 360 milhões de euros de confiança em horas.

André Gouveia: *Há alguma criptomoeda que tenha chamado a sua atenção?*

Miguel Correia: A Polkadot. O interesse não é a moeda em si, mas esta servir para a interoperabilidade entre blockchains diferentes.

André Gouveia: *Os principais bancos centrais estão a estudar projetos de moedas virtuais. Acha que a tecnologia já está madura o suficiente para lhe confiarmos o sistema financeiro?*

Miguel Correia: Sim, penso que a tecnologia está madura, mas ainda é complexa, e não existem engenheiros, em quantidade e com formação adequada, para gerir infraestruturas críticas nela baseadas.

André Gouveia: *Participa em iniciativas nesta área ao nível europeu. Como vê a posição da Europa face aos Estados Unidos e à China?*

Miguel Correia: Na Europa, está a surgir uma blockchain única no mundo: a European Blockchain Services Infrastructure (EBSI). Esta blockchain vai servir para criar serviços para os cidadãos, como um número de Segurança Social europeu ou de notariado.

A EBSI está a ser desenvolvida por um grupo denominado European Blockchain Partnership (EBP). Sou representante nacional no EBP e, atualmente, um dos seus co-chairs, de modo que tenho acompanhado a iniciativa de muito perto.

Estou muito contente por, em breve, estar ativo o primeiro nó português, por iniciativa do



Instituto Politécnico da Guarda, fruto do empenho do Eng.º António Matias Gil. Nem os EUA, nem a China, estão a desenvolver nada semelhante. Isso não é sinal de que estejam atrás da Europa no domínio da blockchain, mas simplesmente não têm interesse em algo como a EBSI.

Ambos têm vantagens tremendas em relação à Europa. Os EUA têm uma cultura de liberdade para inovar e de assumir pessoalmente riscos, que é imbatível. A China tem uma dimensão incomparável. Não é uma coincidência que todas as grandes empresas tecnológicas sejam americanas e que as que vêm a seguir sejam chinesas. É urgente uma mudança de mentalidade em Portugal e na Europa.

André Gouveia: *E, em Portugal, há colaboração entre investigadores e empresas?*

Miguel Correia: A colaboração entre universidade e empresas existe. No Instituto Superior Técnico, temos uma rede de parceiros com mais de 15 grandes empresas. Temos também desenvolvido projetos de blockchain com algumas empresas e alguns organismos públicos.

Os nossos empresários, sem dúvida, mostram interesse no tema. Tenho sido contactado por alguns. Outros frequentaram a primeira edição do curso Blockchain e Smart Contracts, uma parceria entre o Técnico e a Católica Lisbon, que eu coordeno em conjunto com o professor Paulo Amaral, e que foi um sucesso.

André Gouveia: *Há atividades que se podem tornar obsoletas com a maior utilização de blockchains. Quais?*

Miguel Correia: Muitas inovações tecnológicas reduzem a procura de certas profissões e criam outras novas. A blockchain não é diferente. Operações de verificação manuais, como transferências monetárias, vão passar a ser menos necessárias. Pelo contrário, vão ser precisos mais profissionais relacionados com blockchain. É o caso de engenheiros e gestores.