BLOCKCHAIN E CRIPTOMOEDAS

Uma breve análise das suas implicações sociais

Amanda Silva, up201800698@fe.up.pt, Diogo Rodrigues, up201806429@fe.up.pt, Diogo Almeida, up201806630@fe.up.pt, Franscisco Borralho, up201806242@fe.up.pt, Miguel Silva, up201806388@fe.up.pt, Tiago Rocha, up201406679@fe.up.pt

U.PORTO
FEUP FACULDADE DE ENGENHARIA
UNIVERSIDADE DO PORTO

RESUMO

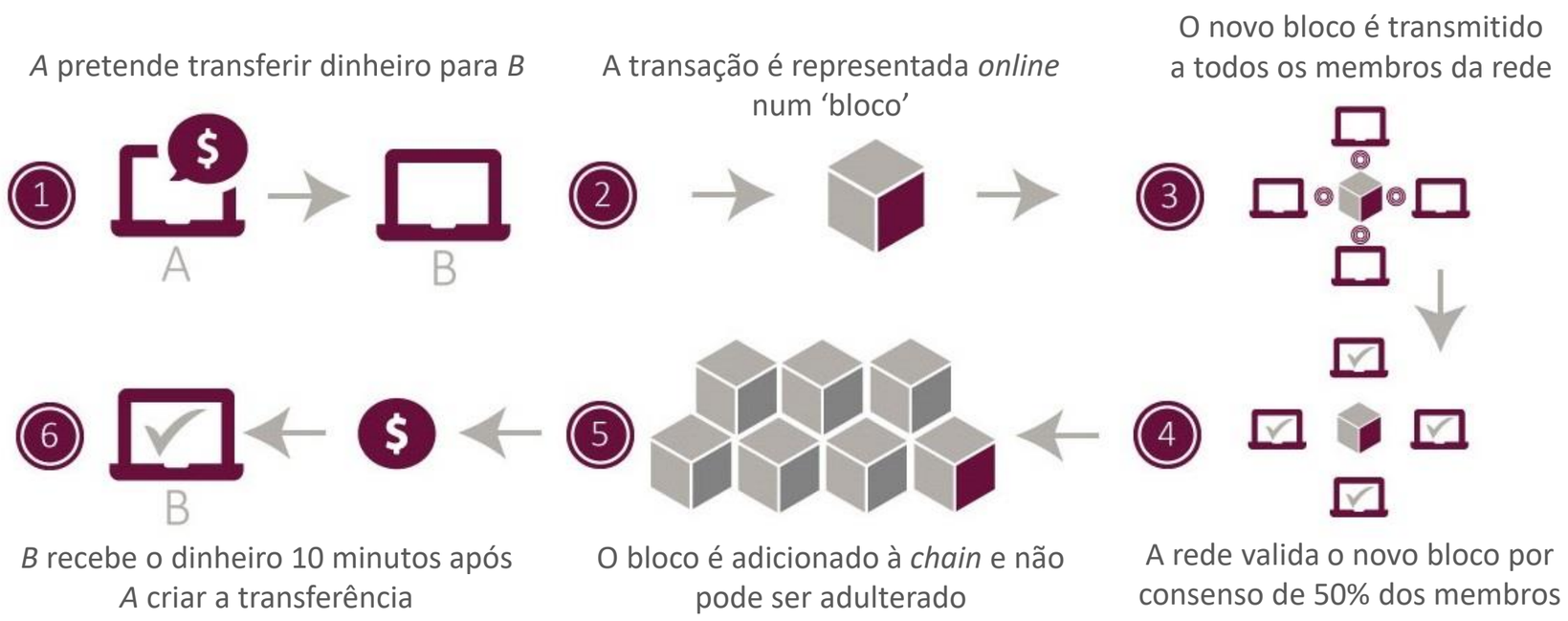
As criptomoedas têm vindo a suscitar o interesse das pessoas por várias razões. Mas, afinal, o que é que torna estas moedas alvo da nossa atenção? Quais as suas implicações sociais? No presente trabalho, são explorados alguns aspetos técnicos das criptomoedas e da *blockchain*, a estrutura de dados que as suporta. Serão também apresentados alguns pontos favoráveis e desfavoráveis às duas tecnologias. Por fim, é exposto um conjunto de aplicações, perspetivas e propostas, particularmente direcionadas à tecnologia da *blockchain*, que se espera que seja utilizada em diversas áreas para além das moedas digitais.

As criptomoedas

As criptomoedas são **moedas virtuais**, cujas transações são guardadas numa *blockchain*, completamente independentes do controlo dos governos, ou qualquer autoridade central. A sua utilização global é facilitada pela sua natureza eletrónica.

A tecnologia *blockchain*

Uma *blockchain* é um **registo público** que armazena todas as transações que ocorrem com, por exemplo, uma criptomoeda. Sempre que ocorre uma transação, o registo continua a crescer, razão pela qual se chama uma cadeia. Esta tecnologia é **descentralizada**, uma vez que a *blockchain* é gerida por um conjunto de computadores com acesso total a toda a informação presente: revisão *peer-to-peer* (P2P).



Vantagens das criptomoedas

- Liberdade financeira
- Moeda descentralizada
- Monitorização em tempo real
- Redução do custo de transações

A ideologia Bitcoin

Quando um banco empresta dinheiro, introduz na economia uma quantidade correspondente de dinheiro, produzindo moeda "do nada". Com a Bitcoin, é possível **remover os bancos e o estado/banco central** do sistema, depositando a confiança em máquinas e protocolos em vez de pessoas, impedindo **interferência excessiva do estado em assuntos pessoais**.

O sistema P2P promove o **horizontalismo social**, pois todos os nodos possuem a mesma autoridade para validar os blocos.

Problemas da Bitcoin

- **Confiança** é transferida para máquinas e protocolos, mas também para gestores de *software* de apoio e empresas de *wallets*.
- **PoW ➤ Concentração de poder** em grupos de desenvolvedores de *software* e *mining pools* (atualmente, 4 *pools* controlam >50% da produção de blocos/moeda, gráfico).
- **Problemas técnicos:** no sistema Bitcoin, dois *forks* e um *bug* crítico (indiciam possíveis problemas no futuro); **ataques informáticos** a cambistas: *e.g.*, o encerramento da *Mt.Gox* deveu-se ao roubo de ₿0.65M (≈US$550M).
- **Problemas legais**: ameaça às moedas soberanas e estados; necessidade de legislação e taxas específicas e difíceis de implementar; o caráter semianónimo permite acesso a bens, serviços e operações ilegais através da *Dark Web*.
- **Volatilidade** e facilidade de especulação dificultam o seu uso como moeda de troca.

Outras aplicações da *blockchain*

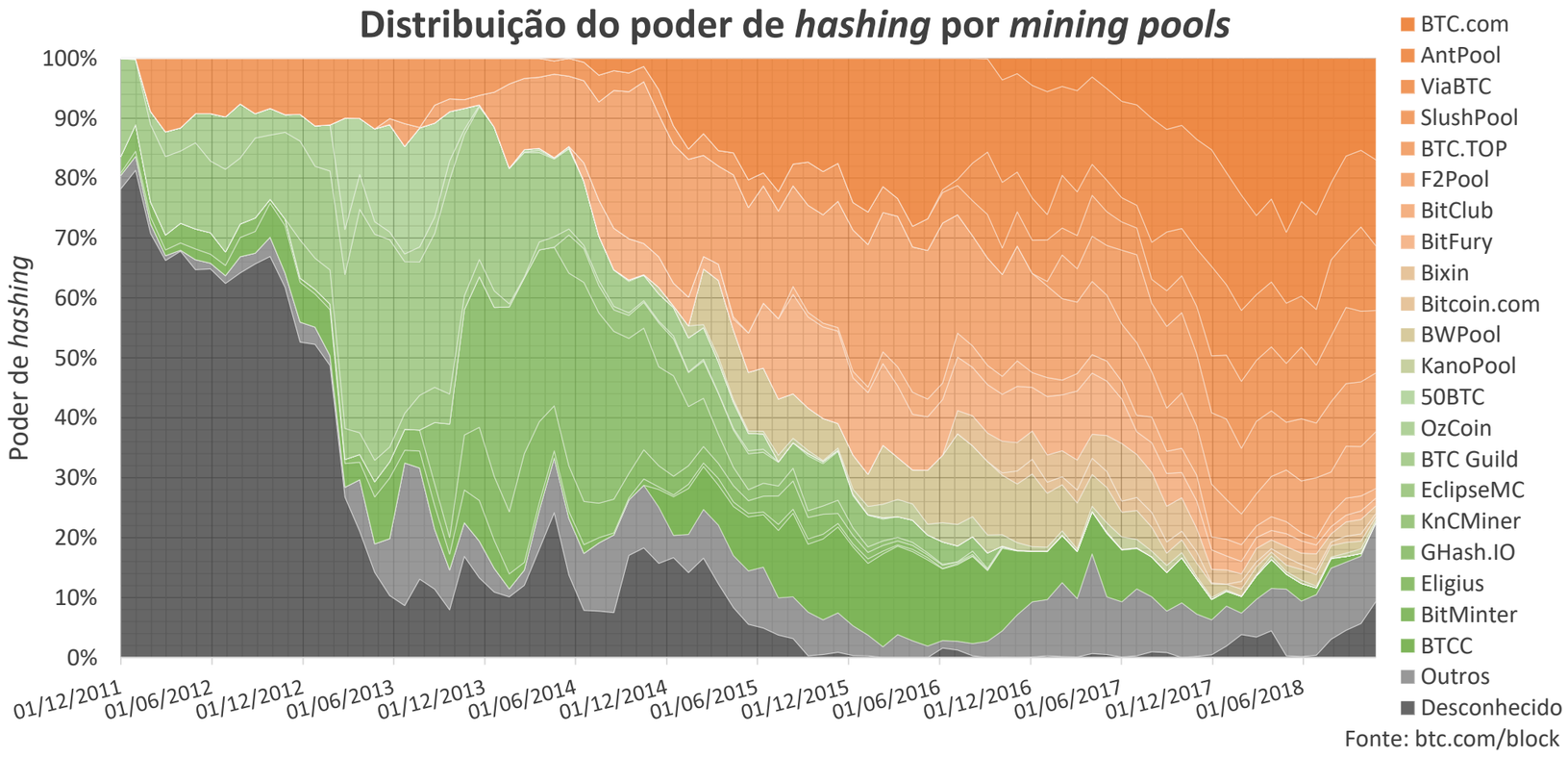
- **Autenticação de documentos:** os registos não se encontram sujeitos a degradação física nem a adulteração passado algum tempo, encontrando-se sempre disponíveis.
- ***Smart contracts***: permitem à rede transferir um montante de uma pessoa para outra quando determinadas condições forem cumpridas.
- **Moeda soberana em formato digital:** com a sua oficialização, a população teria amplo acesso às moedas *tokenizadas*, baseado em *tokens* e no mecanismo de transferên-cia P2P, sem juros, com a privacidade de saldo e transações garantida pelo sigilo bancário tal como nos bancos de hoje, e com custos muito mais baixos.

Implicações sociais da *blockchain*

A *blockchain* é uma boa solução em termos de **privacidade**, visto que o armazenamento da informação é realizado num grande conjunto de máquinas, e **de forma encriptada** como garantia de segurança. No entanto, a ligação entre o utilizador e a transação **pode ser rastreada**, levando à origem da transferência e possivelmente expondo a sua identidade.

Propostas de melhoria da privacidade na *blockchain*

- **P2P *mixing protocols***: utilização de um serviço de *mixing* anónimo para misturar o rasto de transferências/transações e confundir eventuais rastreadores
- ***Distributed mixing networks***: usam protocolos de *mixing*, facilitando também as transações
- **Altcoins:** moedas alternativas à Bitcoin, frequentemente mais seguras (em consequência de experiências passadas), oferecendo mais privacidade e anonimato nas transferências.



Fonte: btc.com/block