



Blockchain

Uma breve análise das criptomoedas e das suas implicações sociais



Projeto FEUP 2018/19 – Mestrado Integrado em Engenharia Informática e Computação:

(nome do coordenador geral)

José Manuel De Magalhães Cruz

Equipa 1MIEIC05_4:

Supervisor: João Correia Lopes

Monitor: Sara Fernandes

Estudantes & Autores:

Amanda Silva up201800698@fe.up.pt Francisco Borralho up201806242@fe.up.pt

Diogo Rodrigues up201806429@fe.up.pt Miguel Silva up201806388@fe.up.pt

Diogo Almeida up201806630@fe.up.pt Tiago Rocha email@email.com

Resumo

[O resumo tem um carácter essencialmente informativo, devendo ser escrito de forma concisa (até 200 palavras) de maneira a captar o interesse de quem o vai ler. Deve incluir os seguintes tópicos: âmbito, objetivos, os métodos, as principais descobertas, incluindo resultados, conclusões e recomendações, se existirem.

Para saber mais sobre como redigir um bom resumo consulte o tutorial online disponível no [website na Biblioteca](#): “[Guia de Apoio à Publicação](#)”, secção: [Estruturar Relatório Técnico](#)]

Palavras-Chave

palavra 1; palavra 2; ...

[as palavras-chave devem ser indicadas logo a seguir ao resumo]

Índice

Lista de figuras	4
Lista de acrónimos.....	5
Glossário	6
1. Introdução.....	7
1. A criptomoeda.....	8
2. A blockchain	9
2.1 Aspetos técnicos da blockchain.....	9
2.2 A utilização da blockchain nas criptomoedas	9
2.3 A ideologia da blockchain.....	9
2.3.1 Descentralização	9
2.3.2 P2P.....	9
2.3.3 Inviolabilidade da blockchain	9
3. Vantagens da utilização das criptomoedas e da Bitcoin.....	10
4. A ideologia Bitcoin	11
4.1 Teoria do dinheiro	11
4.1.1 Bitcoin e a revolução sobre a teoria do dinheiro.....	11
4.2 Cripto-utopia.....	11
4.3 Contradições da ideologia Bitcoin	12
4.3.1 Estrutura social da Bitcoin.....	12
4.4 Problemas legais associados à Bitcoin.....	13
2. Secção - Estilo "Heading 1" = "Título 1"	Erro! Marcador não definido.
2.1.3 Equações.....	Erro! Marcador não definido.
2.1.3 Figuras e tabelas	16
2.1.4 Citações.....	Erro! Marcador não definido.
3. Questões Técnicas	Erro! Marcador não definido.
4. Conclusões.....	19
5. Recomendações.....	Erro! Marcador não definido.
Referências bibliográficas.....	20
Apêndices.....	21

Lista de figuras

Figura 1: Fotografia aérea do Campus da FEUP, campus da FEUP realçado a cor ... 17

Lista de acrónimos

[Elemento opcional.

Justifica-se se estes elementos (acrónimos, unidades, símbolos) ocorrerem com grande frequência no relatório. Quando ocorrerem pela primeira vez no texto deve apresentar-se a respetiva definição.

Para saber mais consulte o tutorial online “[Guia de Apoio à Publicação](#)”.]

Glossário

[Elemento opcional].

Justifica-se sempre que seja necessário esclarecer o leitor sobre o significado de terminologia específica usada no texto no relatório.

Recomenda-se a sua localização nos elementos iniciais, embora na normalização existente haja variantes, podendo também constar nos elementos finais.

Para saber mais consulte o tutorial online “[Guia de Apoio à Publicação](#)”.]

1. Introdução

[Contextualização sucinta do assunto do relatório, fazendo-se referência ao âmbito e aos objetivos. Aqui se clarifica a motivação do trabalho apresentado e se explica a abordagem adotada e a sua relação com trabalhos análogos, numa perspectiva genérica. Não se deve antecipar detalhes sobre o que é explicado nas secções posteriores. Se for pertinente, pode-se indicar ainda qual o público a que se destina.

Para saber mais consulte o tutorial online “[Guia de Apoio à Publicação](#)”.]

2. A criptomoeda

3. A blockchain

3.1 Aspetos técnicos da blockchain

3.2 A utilização da blockchain nas criptomoedas

3.3 A ideologia da blockchain

3.3.1 Descentralização

3.3.2 P2P

3.3.3 Inviolabilidade da blockchain

4. Vantagens da utilização das criptomoedas e da Bitcoin

5. A ideologia Bitcoin

5.1 Teoria do dinheiro

Apesar da teoria do dinheiro não se enquadrar em grande parte no âmbito deste relatório, a compreensão de alguns conceitos fundamentais desta área é essencial ao desenvolvimento do tópico da Bitcoin como motivo de alteração do paradigma económico.

A *reserva bancária* é o conjunto de ativos líquidos de um banco, que lhe permite corresponder à necessidade de levantamentos dos depositantes. Num *sistema de reserva total*, a reserva de um banco corresponde à totalidade dos depósitos, prestando apenas serviços de segurança aos depositantes (Abel, Bernanke, e Croushore 2011).

Mas supondo que os montantes de depósitos e levantamentos se equilibram aproximadamente, e que é improvável que os depositantes pretendam levantar uma grande parte dos depósitos num curto intervalo de tempo (*corrida aos bancos*), o banco necessita de apenas uma fração dos depósitos em reserva (*reserva mínima*) de forma a satisfazer os levantamentos¹. No *sistema de reserva fracional*, o banco pode utilizar a maior parte dos depósitos para conceder empréstimos com juros a clientes com baixo risco de incumprimento, aumentando os seus lucros (Abel, Bernanke, e Croushore 2011). Assim, (1) os depositantes têm a ‘garantia’ de poder efetuar levantamentos², e (2) os devedores recebem dinheiro após contraírem empréstimos. Assim, considera-se que o banco “criou dinheiro a partir do nada”, uma vez que processa (2) enquanto se compromete com (1) (Rothbard 1995).

5.1.1 Bitcoin e a revolução sobre a teoria do dinheiro

5.2 Cripto-utopia

O sucesso da Bitcoin apoia-se no falhanço do sistema económico-financeiro, tanto do ponto de vista ético e moral, como do ponto de vista prático.

A própria noção de moeda *fiat*, cuja produção se encontra intrínseca e sistematicamente associada à **produção de dívida** e ao binómio devedor-credor, prejudica a sua imagem na perspetiva da igualdade de direitos (o credor exige ao devedor a restituição do valor da dívida), assim como incomoda quem considera a dívida um problema moral, económico e político (Dodd 2017).

A utilização da Bitcoin visa, além da substituição do atual sistema financeiro, a remoção de dois principais intermediários: os bancos, e o estado (Dodd 2017).

¹ Por exemplo, a Reserva Federal dos EUA exige uma reserva mínima de 10% a bancos com total de operações >\$122,3M (Federal Reserve 2017), e o BCE exige 1% (European Central Bank 2018).

² Mesmo que um banco declare insolvência, o banco central possui um fundo de garantia de depósitos, para o qual contribuem todos os bancos, que garante o pagamento aos depositantes.

Para (Rothbard 1995), **o sistema de reserva fracional é inerentemente insolvente**, uma vez que um banco depende da ignorância dos depositantes para os convencer de que o dinheiro depositado se encontra de facto “no banco”. Se os depositantes se apercebessem da realidade, ocorreria uma corrida aos bancos e consequente insolvência de múltiplos bancos. Nessa situação, seria impossível resgatar o sistema financeiro com todo o dinheiro que existe, forçando o banco central a emitir moeda suficiente para pagar a todos os depositantes, provocando hiperinflação.

A ideia de uma moeda como a Bitcoin traduz o objetivo de remover os bancos do sistema financeiro, uma vez que se extinguem as funções de salvaguardar dinheiro ou produzi-lo através de criação de dívida. A Bitcoin possui **valor real** na medida em que representa o custo de hardware, computacional, e energético de a produzir (Maurer, Nelms, e Swartz 2013), além de ser dinheiro totalmente desligado de dívida, espelhando características geralmente apontadas ao ouro quando usado como moeda-mercadoria (Dodd 2017). O próprio vocabulário da Bitcoin traduz o paralelismo com o ouro, por exemplo nos termos *miners/mining* e *rigs*; inclusive em (Nakamoto 2009), é estabelecida a comparação entre a Bitcoin e o ouro:

“A adição gradual de uma quantidade constante de moedas é análoga ao gasto de recursos pelos mineiros de ouro para adicionar ouro à circulação. No nosso caso, são gastos tempo de CPU e eletricidade”.

A ideia de uma moeda descentralizada apela aos anti-estado.

Além do sistema de reserva fracional ser falhado, coloca os bancos no topo da hierarquia como produtores de dinheiro.

5.3 Contradições da ideologia Bitcoin

Grande parte da atenção pública atraída pela Bitcoin está associada à volatilidade do seu valor e das taxas de câmbio. Apesar da Bitcoin poder ser utilizada na aquisição de bens, os preços encontram-se tabelados em outras moedas como o dólar americano ou o euro (Dodd 2017), um processo que torna a Bitcoin num intermediário da transação, utilização contrária ao objetivo fundamental de se tornar numa moeda presente integralmente na transação.

5.3.1 Estrutura social da Bitcoin

De acordo com (Dodd 2017), “é fácil exagerar o impacto da Bitcoin fora dos círculos de aficionados”. O relatório de (Agrawal 2015) sobre os resultados da sondagem do Coin Center até março de 2015 revelaram que 35% dos inquiridos se encontravam familiarizados com a Bitcoin, e que apenas 4,5% tinham usado a moeda digital. A análise de (Brown 2018) aos

resultados da sondagem da LendEDU, de agosto de 2017, salienta o crescimento da consciência pública sobre a Bitcoin (78,6%), apesar da reduzida utilização reportada pelos inquiridos (11,0%)³.

5.4 Problemas legais associados à Bitcoin

³ Note-se que (Agrawal 2015) e (Brown 2018) se reportam a sondagens *online*, pelo que existem limitações na generalização das inferências de ambas as sondagens à população em geral. A utilização de uma metodologia de correção de resultados é referida explicitamente apenas na sondagem do Coin Center por (Valkenburgh 2015).

6. Aplicações da blockchain em outros domínios

6.1 Moeda oficial pública

6.2 Extinção de cartórios

6.3 Smart contracts

6.4 Bases de dados

6.4.1 Aplicações da blockchain à saúde

6.4.2 Aplicações da blockchain à indústria

6. Implicações sociais da blockchain

6.1 Direito digital

6.2 Privacidade

6.3 Mudança de paradigmas

Este texto é apenas um exemplo que precede uma equação.

Equações simples podem ser inseridas em linha com o texto, a reta é $y = mx + b$.

Equações mais complicadas devem ser separadas em linhas individuais e numeradas sequencialmente à direita dentro de parêntesis. Esta é a equação 2º grau genérica:

$$ax^2 + bx + cx = 0 \tag{1}$$

Todos os coeficientes devem ser definidos de forma sistemática tal como por exemplo

Onde: a é o coeficiente de 2º grau; b o de 1º grau; c o coeficiente independente da variável x, a determinar.

As equações devem ser referidas mantendo o número e parêntesis. Por exemplo a equação (2) resolve problemas formulados tal como mostrado em (1).

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \tag{2}$$

Para obter aspeto uniforme, copiar e alterar a linha acima e atualizar o número da equação.

2.1.3 Figuras e tabelas

Todas as figuras e tabelas devem ser obrigatoriamente legendadas e numeradas sequencialmente:

- as figuras devem ser legendadas por baixo;
- as tabelas devem ser legendadas no topo.

Mantenha as figuras centradas e em linha com o texto para que a legenda apareça sempre colada com a imagem. No documento final não deixe grandes espaços em branco, se necessário troque de ordem parágrafos de texto com figuras de modo a ocupar a quase totalidade da folha utilizável.

Como exemplo, a figura 1 mostra o campus da FEUP.



Figura 1: Fotografia aérea do Campus da FEUP, campus da FEUP realçado a cor

A Tabela 1 serve para exemplificar como mostrar alguns valores que neste caso têm a ver com alguns dados numéricos associados a recursos e investimentos da FEUP no ano de 2011.

Tabela 1: Recursos Físicos da FEUP (excerto adaptado de “A FEUP em números”, 2011)

Área total do campus FEUP	93 918 m ²
Espaços verdes	23 000 m ²
Número de computadores dedicados ao ensino	1 815
Investimento em equipamentos de laboratório	1,46 M€

À medida que escreve o texto do relatório deve indicar os trabalhos de outros autores em que se baseia, sob a forma de citações. Isto consiste em indicar de forma abreviada as fontes usadas às quais foi buscar informação adicional para desenvolver o tema do seu relatório.

Existem duas formas principais de citar:

- por paráfrase: interpretação do conteúdo original por palavras diferentes das da fonte consultada, indicando a fonte logo a seguir.
- ou
- por transcrição: uso de um excerto do conteúdo original apresentando-o entre aspas, indicando a fonte logo a seguir.

As citações devem obedecer a um estilo normalizado. De entre os muitos que existem, a Biblioteca da FEUP aconselha o estilo Chicago (formato autor-data). Na caixa abaixo exemplifica-se uma citação (por paráfrase) de acordo com esse estilo:

A decisão de escolha de um tema para um trabalho académico pode variar. O tema pode ser

pensado e escolhido pelo próprio estudante, ou a partir de uma lista de temas já concebidos, com potencial interesse para estudo. **(Bell, 2002)**

A cada citação ao longo do texto deve corresponder uma referência indicada na lista final de referências bibliográficas.

É importante não esquecer que também as figuras (imagens, tabelas, gráficos, etc.) provenientes de obras de outros autores (por exemplo obtidas através da Internet) devem ser citadas sempre, após as respectivas legendas.

Para saber mais sobre este assunto e ver exemplos, consulte o guia “[Evitar o plágio: normas para citar e referenciar](#)”.

A inserção de citações e referências pode ser feita de forma automática usando ferramentas como o Endnote ou o Mendeley, entre outros. Para saber mais sobre estas ferramentas consulte o guia “[Criar Bibliografias: Ferramentas citar e organizar referências](#)”.

7. Conclusões

[Apresentação clara e organizada das deduções ou ilações extraídas após a discussão dos resultados do estudo, como forma de responder à pergunta inicial do projeto. Por esse motivo não deve ser um texto de detalhe, nem um texto em que se apresente algo de novo, mas um texto de afirmação que deve ser lido de forma independente do restante relatório.

Para saber mais consulte o tutorial online “[Guia de Apoio à Publicação](#)”.]

Referências bibliográficas

- Abel, Andrew B., Ben S. Bernanke, e Dean Croushore. 2011. *Macroeconomics*. 7 ed, *The Pearson Series in Economics*. Boston: Pearson Education, Inc.
- Agrawal, Neeraj. 2015. "Coin Center releases March 2015 Bitcoin Public Sentiment Survey Data." Coin Center, Atualizado em 31 de março de 2015, acessado em 14 de outubro de 2018. <https://coincenter.org/entry/coin-center-releases-march-2015-bitcoin-public-sentiment-survey-data>.
- Brown, Mike. 2018. "Bitcoin's Present (and Future) Role in the American Economy." LendEDU, Atualizado em 23 de agosto de 2018, acessado em 10 de outubro de 2018. <https://lendedu.com/blog/bitcoins-role-in-the-american-economy/>.
- Dodd, Nigel. 2017. "The Social Life of Bitcoin." *Theory, Culture and Society* 35 (3):35-56. doi: 10.1177/0263276417746464.
- European Central Bank. 2018. "How to calculate the minimum reserve requirements." Atualizado em 2018, acessado em 15 de outubro de 2018. <https://www.ecb.europa.eu/mopo/implement/mr/html/calc.en.html>.
- Federal Reserve. 2017. "Policy Tools: Reserve Requirements." Atualizado em 3 de novembro de 2017, acessado em 15 de outubro de 2018. <https://www.federalreserve.gov/monetarypolicy/reservereq.htm>.
- Maurer, Bill, Taylor C. Nelms, e Lana Swartz. 2013. "'When perhaps the real problem is money itself!': the practical materiality of Bitcoin." *Social Semiotics* 23 (2):261-277. doi: 10.1080/10350330.2013.777594.
- Nakamoto, Satoshi. 2009. "Bitcoin: A Peer-to-Peer Electronic Cash System." *Cryptography Mailing list* at <https://metzdowd.com>, <https://bitcoin.org/bitcoin.pdf>.
- Rothbard, Murray N. 1995. "Fractional Reserve Banking." *The Freeman* 45 (10):624-627, <https://mises.org/library/freeman-1995>.
- Valkenburgh, Peter Van. 2015. "Coin Center's new Bitcoin Public Sentiment Survey." Coin Center, Atualizado em 27 de janeiro de 2015, acessado em 14 de outubro de 2018. <https://coincenter.org/entry/coin-center-s-new-bitcoin-public-sentiment-survey>.

Apêndices

[Elemento opcional.

Os apêndices e os anexos contêm informação que complementa, apoia e clarifica o relatório e cuja inclusão no corpo principal do relatório interferiria com uma boa ordem de apresentação das ideias.

Há uma diferença importante entre apêndices e anexos. Para saber mais consulte o tutorial “[Guia de Apoio à Publicação](#)”.]

Apêndice A

Apêndice B