DATA PROTECTION

PEDRO MARTINS

INTRODUÇÃO À BLOCKCHAIN

BITCOIN, CRIPTOMOEDAS, SMART CONTRACTS, CONCEITOS, TECNOLOGIA, IMPLICAÇÕES

FCA

Edição
FCA – Editora de Informática, Lda.
Av. Praia da Vitória, 14 A – 1000-247 Lisboa
Tel: +351 213 511 448
fca@fca.pt
www.fca.pt

Distribuição
Lidel – Edições Técnicas, Lda.
Rua D. Estefânia, 183, R/C Dto. – 1049-057 Lisboa
Tel: +351 213 511 448
lidel@lidel.pt
www.lidel.pt

Livraria
Av. Praia da Vitória, 14 A – 1000-247 Lisboa
Tel: +351 213 511 448 * Fax: +351 213 522 684
livraria@lidel.pt

ISBN edição impressa: 978-972-722-887-4
1.ª edição impressa: março 2018

Paginação: Carlos Mendes
Impressão e acabamento: Cafilesa – Soluções Gráficas, Lda. – Venda do Pinheiro
Depósito Legal n.º 438378/18
Capa: José M. Ferrão – *Look-Ahead*

Para a Rita, o Francisco e a Constança

O AUTOR

Pedro Martins é Diretor de TI/SI no NOVO BANCO e Vice-Presidente da Associação Portuguesa de Data Science. Trabalhou para grandes multinacionais de consultoria, tendo executado variados projetos de TI/SI para diversas empresas financeiras, de telecomunicações e de energia.

Licenciado em Engenharia Física Tecnológica pelo Instituto Superior Técnico (IST), pós-graduado em Governança dos Sistemas de Informação pelo Instituto Superior de Economia e Gestão (ISEG) e mestrando em Informação e Sistemas Empresariais no IST.

ÍNDICE

Agradecimentos IX

Prefácio XI

Introdução XIII

PARTE I – A Confiança, a Criptografia e o Dinheiro Criptográfico 1

1 A Importância da Confiança e o Desafio da Descentralização 3

2 Conceitos Fundamentais de Criptografia 17

3 Das *Commodities* ao Dinheiro Criptográfico 31

PARTE II – A Tecnologia Blockchain 51

4 A Bitcoin e a Tecnologia Blockchain 53

5 Indo Além da Bitcoin: Altcoins, Ethereum e Blockchain 2.0 103

6 Exemplos de Aplicabilidade da Tecnologia Blockchain 121

PARTE III – O Despontar de uma Nova Era 135

7 Implicações Económicas, Sociais, Políticas 137

Considerações Finais 153

Bibliografia 157

Índice Remissivo 159

AGRADECIMENTOS

A escrita de um livro é geralmente um ato solitário praticado pelo autor, mas a sua concretização é sempre o resultado do trabalho coletivo das várias pessoas que a ele se dedicaram e sem as quais o livro não se tornaria uma realidade.

É, portanto, da mais elementar justiça fazer o reconhecimento e o agradecimento públicos às seguintes pessoas, na certeza de que, sem o seu profissionalismo, competência e dedicação, e em muitos casos abnegação, a feitura deste livro não teria sido possível.

Agradeço ao Eng.º Frederico Annes e à Dr.ª Sandra Correia, respetivamente Diretor Editorial e Editora Adjunta da FCA – Editora de Informática, o entusiasmo com que acolheram desde a primeira hora esta proposta editorial e todo o apoio que prestaram em todas as fases da escrita e da produção deste livro. Agradeço à Ana Correia, Assistente Editorial da FCA – Editora de Informática, pelo seu elevado profissionalismo e empenho, e à Raquel Rua Oliveira, ao Carlos Mendes e ao José M. Ferrão, pelos trabalhos de revisão, paginação e *design*, respetivamente.

Agradeço ao Professor Miguel Pupo Correia a gentileza de ter aceitado prefaciar esta obra e dessa forma ter dado um contributo inestimável para a qualidade da mesma.

Agradeço ao Bernardo Fialho, ao Luís Dieb, ao Nuno Correia e ao Rui Fonseca por terem tido a paciência de ler e comentar os excertos do livro que lhes fui apresentando.

Por último, um agradecimento especial à Rita, minha mulher, ao Francisco e à Constança, meus filhos, por terem compreendido e aceitado a minha menor disponibilidade durante os meses de escrita deste livro.

PREFÁCIO

Apesar de recente, a tecnologia Blockchain está a atrair imensa atenção em todo o mundo. Qualquer tecnologia informática para ter sucesso precisa de uma *killerapp*, ou seja, de uma aplicação apelativa que promova a sua adoção. Muitas tecnologias falharam por não terem uma *killerapp*. Uma vantagem da Blockchain é ter pelo menos duas.

A primeira *killerapp* da Blockchain foi também a sua primeira aplicação: as criptomoedas. O termo Blockchain surgiu no contexto do bitcoin, a primeira e mais conhecida criptomoeda. A Blockchain original não era mais do que o núcleo da Bitcoin, o registo das transações efetuadas usando bitcoins. O sucesso desta ideia foi de tal ordem que, hoje em dia, existem centenas de criptomoedas, com um valor total superior a 200 mil milhões de euros, cerca de metade devido à Bitcoin.

A segunda *killerapp* são os *smart contracts*, ou seja, contratos informáticos programados e executados de forma semelhante a qualquer outro *software*. Esta ideia de criar contratos que têm uma semântica inequívoca, pelo facto de serem programados, e cuja execução será realizada necessariamente como especificado tem, com justiça, atraído uma enorme atenção. O potencial que tem para revolucionar a forma de interação entre empresas e outras organizações ou, até mesmo, o funcionamento da justiça, é inegável. Um dinâmico ecossistema de *startups* financeiras, denominadas *fintechs*, está a fervilhar em consequência deste potencial.

Estes dois campos de aplicação só são viáveis se for possível ter confiança na infraestrutura informática que os sustenta. A tecnologia Blockchain fornece precisamente infraestruturas que permitem ter essa confiança. Uma Blockchain é um registo, um livro de razão, ao qual se podem acrescentar itens, mas não alterar os que aí se encontram ou modificar a sua ordem. A confiança de que essas propriedades de facto se verificam é baseada, por um lado, na utilização de um grupo de vários computadores – possivelmente dezenas, centenas ou até milhares – para armazenar esse registo e executar as operações que ele permita. Por outro lado, essa confiança é baseada na utilização de um conjunto de mecanismos criptográficos.

Esta obra surge em boa hora, quando começam a surgir aplicações práticas da tecnologia Blockchain para além das criptomoedas, já que o interesse no tema é crescente e ainda não existem textos disponíveis na nossa língua.

A obra trata de um tema complicado usando uma linguagem acessível. Começa pelo começo: pelas noções de confiança e descentralização. Os outros capítulos da primeira parte abordam outros temas introdutórios: conceitos básicos de criptografia e as formas de dinheiro eletrónico pré-Bitcoin. A segunda parte do livro, a mais extensa, apresenta em detalhe a tecnologia Blockchain. Começa pela Bitcoin e pela Blockchain original. O capítulo seguinte apresenta as altcoins, os *smart contracts* e a Ethereum, uma das mais populares Blockchains. O terceiro capítulo desta parte explora diversos casos em que pode ser interessante utilizar esta tecnologia. A terceira e última parte conclui o livro, não sem antes apresentar um exercício de previsão sobre o impacto da Blockchain na economia e na sociedade.

Recomendo, portanto, a leitura atenta desta obra na qual se pode fazer uma primeira descoberta deste admirável mundo novo da Blockchain!

Lisboa, 27 de novembro de 2017

Miguel Pupo Correia
Professor Associado – INESC-ID,
Instituto Superior Técnico,
Universidade de Lisboa

INTRODUÇÃO

Decidi escrever este livro de introdução à tecnologia Blockchain por duas razões principais. A primeira, de natureza intelectual e profissional, por constatar a extrema importância desta nova tecnologia e pela necessidade de organizar conhecimentos e proporcionar uma visão panorâmica sobre a sua utilidade, aplicabilidade e potencial para a inovação. A segunda, por constatar a escassez no mercado editorial português e em língua portuguesa, da necessária e urgente bibliografia introdutória à tecnologia Blockchain, que descreva e explique em linguagem simples e de forma acessível os principais conceitos e forma de funcionamento desta invenção, a qual se apresenta aos olhos de muitos como instigadora de profundas transformações tecnológicas e económicas e, aos olhos de outros, mais otimistas, também de profundas transformações sociais e políticas.

A tecnologia Blockchain pode ser empregue na criação de sistemas de registo inovadores, na criação e transação de novas classes de ativos digitais, na criação de inovadores sistemas de incentivos comunitários e na automatização de processos. Fá-lo prescindindo das tradicionais instituições intermediárias em quem, ao longo de séculos, temos vindo a depositar a nossa confiança na capacidade para garantir e gerir o correto funcionamento dos sistemas económicos, sociais e políticos.

Ao reinventar a forma como lidamos com contratos, transações e sistemas de registo, elementos estruturais das organizações económicas, sociais e políticas, a tecnologia Blockchain poderá ser indutora de extensíssimas transformações nas mais variadas áreas da atividade humana. Privilegiando e facilitando a criação de redes globais e transparentes de relacionamento direto e mais eficiente entre agentes, a tecnologia Blockchain poderá vir a ser um importante catalisador dessas transformações, conduzindo-nos porventura a uma nova era mais igualitária, inclusiva, transparente e descentralizada.

Se a tecnologia Blockchain virá a ser o Santo Graal que muitos anteveem e desejam, apenas o tempo o dirá. O que sabemos hoje é que esta tecnologia, que nasceu no ano de 2009 com a invenção da Bitcoin, mas cujo alcance vai

muito além das moedas virtuais, constitui um avanço tecnológico de extrema importância, eventualmente comparável ao surgimento da rede Internet com todas as consequências tecnológicas, económicas, sociais e políticas que daí advieram.

Um avanço tecnológico perseguido durante décadas por investigadores nas áreas da criptografia, dinheiro digital e computação distribuída, responsável pela criação de milhares de novas empresas de base tecnológica, pela captação de vários milhares de milhões de euros para o desenvolvimento de ideias e produto, pelo despertar das chamadas organizações incumbentes para a necessidade de compreensão da tecnologia e identificação de formas úteis de adoção, pelo surgimento das primeiras soluções comerciais inovadoras e disruptivas (como, por exemplo, soluções de pagamentos diretos), e pelo florescimento de uma nova e pujante economia, a economia Blockchain.

Um avanço tecnológico cujo potencial disruptivo sobre os atuais modelos de negócio e formas tradicionais de organização e de gestão, fundamentado pela natureza descentralizada da tecnologia e pela nova arquitetura de plataformas computacionais que introduz, não pode deixar nenhuma organização e nenhum dos seus gestores e responsáveis indiferentes ao seu aparecimento.

Também o cidadão comum não pode ficar indiferente a este avanço tecnológico, pois, tal como a invenção da Internet veio mudar profundamente a forma como nos relacionamos uns com os outros e com as instituições – veja-se por exemplo o uso do e-mail, das redes sociais, ou do *online banking* –, a invenção da tecnologia Blockchain mudará a forma como se cria, obtém e utiliza dinheiro, a forma como se transacionam bens e serviços, a forma como se criam e gerem organizações, e a forma como se participa em sociedade.

Foi a pensar nesta diversidade de leitores que escrevi este livro de introdução à tecnologia Blockchain. Trata-se, por essa razão, de um livro orientado à divulgação da tecnologia, focado na descrição e explicação do essencial da sua forma de funcionamento, que recorre a uma linguagem simples e acessível a todos.

É, portanto, um livro de cariz não técnico, no sentido em que nele o leitor não encontrará, por exemplo, a explicação das bases matemáticas que sustentam as principais operações criptográficas empregues na tecnologia ou exemplos de programação informática. O leitor interessado em aprofundar esses aspetos técnicos poderá complementar esta leitura com a bibliografia adicional sugerida no final do livro.

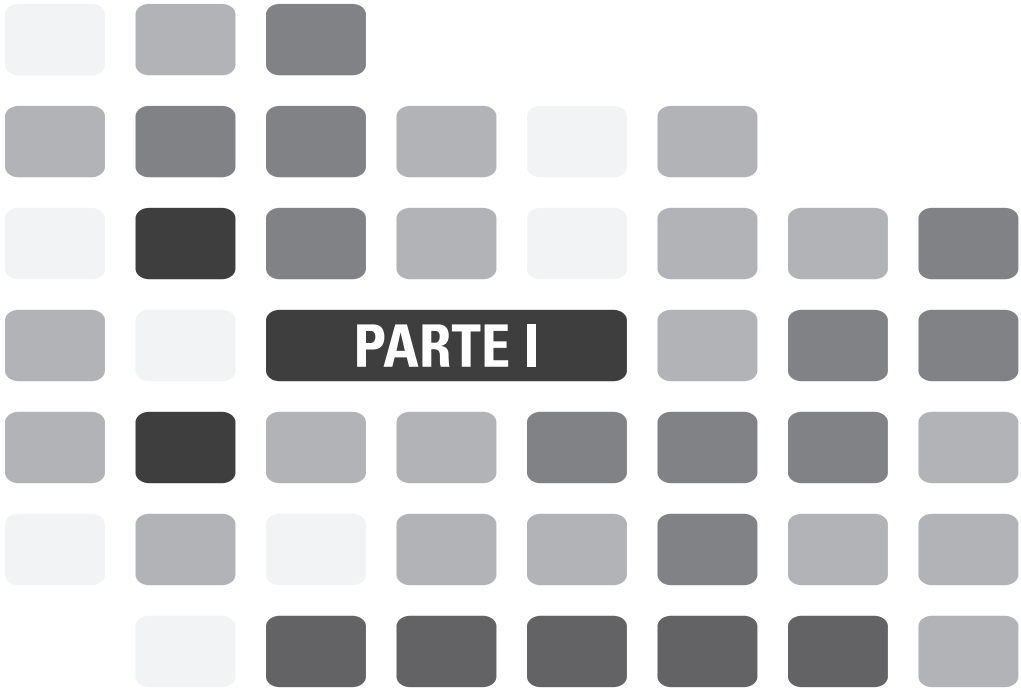
Contudo, para verdadeiramente compreender a inovação proposta por esta nova tecnologia, a sua importância e o seu alcance, o leitor terá de compreender como

esta invenção funciona também a um nível técnico. Este foi o derradeiro desafio na escrita deste livro e, porventura, simultaneamente, o maior prazer. O desafio de conseguir explicar, por palavras e metáforas simples, uma matéria que, por vezes, pode ser tecnicamente muito complexa.

Espero sinceramente que o leitor obtenha com a sua leitura o mesmo prazer que obtive com a sua escrita.

Pedro Martins

A **CONFIANÇA**, A **CRIPTOGRAFIA** E O **DINHEIRO CRIPTOGRÁFICO**



1

A **IMPORTÂNCIA** DA **CONFIANÇA** E O **DESAFIO** DA **DESCENTRALIZAÇÃO**

Confiança
Relações de confiança
Intermediação
Descentralização

"Se as redes alguma vez se puderem tornar mais eficientes [...] isso só será conseguido através de altos níveis de confiança e da existência de normas de conduta ética partilhadas pelos membros das redes."

Francis Fukuyama, cientista político americano

1.1 O QUE SIGNIFICA CONFIAR E COMO SE ESTABELECEM RELAÇÕES DE CONFIANÇA

O que significa confiar?

Uma definição comummente aceite diz-nos que confiar corresponde ao ato de julgamento subjetivo que um agente faz sobre a probabilidade de outro agente ter um determinado comportamento, quando colocado perante uma situação específica e sujeito a determinadas circunstâncias. Confiar significa, portanto, uma certa crença num comportamento, uma expectativa de resultado, expectativa essa tanto mais convicta quanto mais conhecimento se detenha do agente em quem se pretende confiar. Confiar pressupõe, assim, uma necessidade de aquisição prévia de conhecimento sobre o agente no qual se pretende confiar.

Num sistema composto por vários agentes, a soma da confiança acumulada pelos diferentes agentes, isto é, o nível de confiança presente no sistema, depende da maior ou menor capacidade que cada agente tem para adquirir o conhecimento necessário à formulação de uma expectativa de comportamento dos restantes agentes, e das condicionantes sistémicas desse comportamento.

Será mais fácil o estabelecimento de confiança nos sistemas onde a aquisição de conhecimento pelos agentes esteja mais facilitada, do que nos sistemas onde essa aquisição esteja mais dificultada.

É mais fácil o estabelecimento de confiança num sistema com fronteiras bem definidas, em que se conheçam todos os seus agentes e todas as variáveis internas e externas que determinam o seu comportamento, do que nos sistemas em que não se verifiquem todas estas condições. Os sistemas com as características dos primeiros dizem-se sistemas fechados e os sistemas que não verifiquem todas essas condições dizem-se sistemas abertos.

Os sistemas fechados, pelas suas características, tendem a ser naturalmente mais facilitadores do estabelecimento de confiança do que os sistemas abertos, porque tendem a determinar um custo de aquisição de conhecimento comportável pelos seus agentes. Veja-se, por exemplo, a maior facilidade de estabelecimento de confiança que se observa entre os habitantes de uma pequena aldeia, quando comparada com a maior dificuldade de o fazer numa grande metrópole.

1.1.1 Método da relação de confiança direta

Se confiar significa ter uma expectativa de comportamento, uma relação de confiança corresponde ao emparelhamento das expectativas de comportamento de dois ou mais agentes quando colocados perante a mesma situação específica.

A forma mais simples de estabelecer uma relação de confiança é através da aquisição recíproca de conhecimento diretamente entre agentes. Porque a relação de confiança se estabelece diretamente entre os agentes, sem a intervenção de terceiros, designamos este método por método da relação de confiança direta (Figura 1.1).

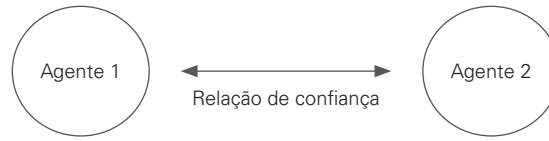


Figura 1.1 • Relação de confiança direta

Este tipo de confiança está presente em inúmeras situações quotidianas, ainda que, por hábito, não tomemos consciência da sua presença. Por exemplo, nos sistemas familiares e nos sistemas de amizade, a forma preponderante de confiança é a direta. Quando os filhos estão doentes e os pais os deixam ao cuidado dos avós no período em que estão a trabalhar, mais não estão a fazer do que a utilizar relações de confiança direta. O mesmo sucede quando alguém empresta o seu automóvel a um amigo para que este possa realizar uma viagem de que necessita.

Os sistemas fechados, onde o custo de aquisição de conhecimento é relativamente mais baixo, constituem um espaço privilegiado para a utilização deste tipo de método de estabelecimento de confiança. Neste tipo de sistemas o conhecimento pode ser adquirido de forma direta e recíproca por todos os agentes, pelo que todos podem estabelecer relações de confiança direta entre si (Figura 1.2).

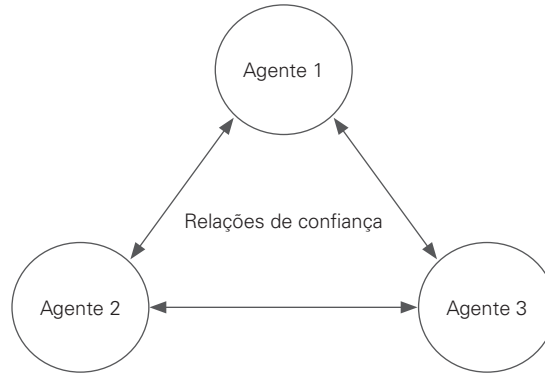


Figura 1.2 • Sistema com relações de confiança direta

O método da relação de confiança direta caracteriza-se ainda por ser simétrico, isto é, igualitário na distribuição de poder entre agentes, no sentido em que todos os agentes detêm o mesmo nível de autonomia e de independência na gestão das suas relações de confiança (Figura 1.3). Com o método da relação de confiança direta, todos os agentes têm igual poder para determinar com quem, quando e em que circunstâncias iniciarão uma relação de confiança, e quando a terminarão.

Figura 1.3 • Distribuição simétrica de poder entre agentes

O método da relação de confiança direta não é, contudo, aplicável a todo o tipo de sistemas. Apesar de ser aplicável a sistemas fechados, a sua aplicabilidade decresce à medida que a dimensão desses sistemas cresce. Isso sucede porque à medida que o sistema cresce torna-se incomportável a todos os agentes, por razões de custo, estabelecerem relações de confiança direta com todos os restantes agentes presentes no sistema (Figura 1.4). Por último, o método da relação de confiança direta também não é geralmente eficaz quando aplicado a sistemas abertos.

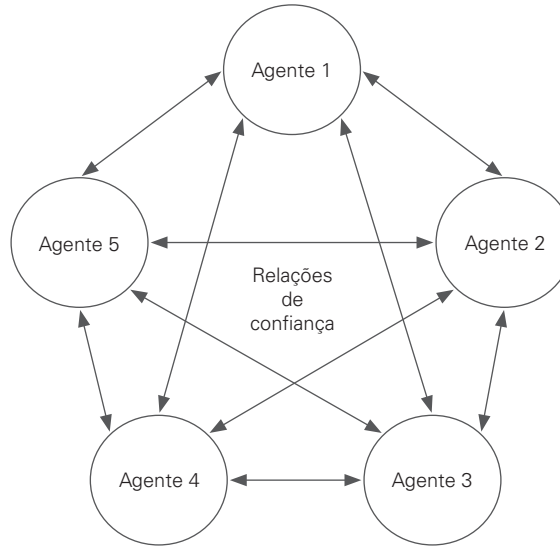


Figura 1.4 • Dificuldade de escalabilidade num sistema com relações de confiança direta

1.1.2 Método da relação de confiança intermediada

Para resolver este problema de escalabilidade verificado no método da relação de confiança direta surgiu um outro método, designado por método da relação de confiança intermediada.

Enquanto no método da relação de confiança direta todos os agentes estabelecem relações de confiança direta e reciprocamente entre si – o que deixa de ser economicamente viável em sistemas de grande dimensão e complexidade –, no método da relação de confiança intermediada os agentes estabelecem uma única relação de confiança. Essa relação de confiança é estabelecida com um agente especial, chamado intermediário, e é através desse intermediário que os agentes estabelecem, indiretamente, relações de confiança (Figura 1.5).

Com o método da relação de confiança intermediada, um agente incorre apenas no custo de estabelecimento de uma relação de confiança com o intermediário, e confia que este estabelece e gere, com os restantes agentes, as necessárias relações de confiança (Figura 1.6). Desta forma, os agentes não têm de suportar o custo de estabelecimento de relações de confiança direta com todos os restantes agentes, como sucederia se recorressem ao método da relação de confiança direta. Por esta razão, o método da relação de confiança intermediada é economicamente mais

2 CONCEITOS FUNDAMENTAIS DE CRIPTOGRAFIA

Cifragem
Criptografia simétrica
Criptografia assimétrica
Função de *hash*
Assinatura digital

"Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação [...]."

Artigo 12 da *Declaração Universal dos Direitos do Homem*

2.1 CRIPTOGRAFIA E OS SEUS PROBLEMAS FUNDAMENTAIS

A criptografia é um ramo da Matemática que se dedica ao estudo dos princípios e das técnicas para a construção de sistemas capazes de providenciar maneiras seguras de tratar informação, isto é, sistemas capazes de transformar uma mensagem inteligível por todos numa mensagem inteligível apenas por uma pessoa ou um conjunto de pessoas autorizadas. Estes sistemas, denominados sistemas criptográficos, procuram dar resposta ao tipo de desafios presentes na seguinte situação.

Imagine-se que duas pessoas, a Ana e o Carlos, pretendem trocar mensagens entre si de forma confidencial através de um canal público, isto é, um canal também acessível a outras pessoas, e que ambos estão impossibilitados de se observarem um ao outro. De que forma pode a Ana assegurar-se que a mensagem que recebe provém de facto do Carlos, e vice-versa? Isto é, como podem ambos assegurarem-se da autenticidade das mensagens trocadas? Adicionalmente, como podem ambos assegurarem-se que as mensagens que trocam entre si não são lidas por mais ninguém e que não são adulteradas? Ou seja, como podem a Ana e o Carlos assegurarem-se da confidencialidade e da integridade das suas mensagens?

Autenticidade, confidencialidade e integridade de mensagens são problemas fundamentais sobre os quais a criptografia se debruça, problemas que têm vindo a merecer diferentes tipos de solução ao longo dos tempos.

As técnicas utilizadas na antiguidade, em particular as de confidencialidade, eram técnicas simples, que consistiam na substituição e transposição dos carateres da mensagem tornando-a ininteligível para quem não conhecesse a regra de transformação aplicada. Um exemplo deste tipo de técnica é o codificador de Atbash, uma técnica de transposição usada pelos hebreus entre 600 a.C. e 500 a.C., que consistia na inversão da sequência de letras do alfabeto, substituindo a primeira letra pela última, a segunda pela penúltima, e assim sucessivamente.

Aplicado ao alfabeto romano, o codificador de Atbash corresponde à aplicação da seguinte regra de substituição:

Normal:	a b c d e f g h i j k l m n o p q r s t u v w x y z
Modificado:	z y x w v u t s r q p o n m l k j i h g f e d c b a

Este tipo de técnica era realizado manualmente e, pela sua simplicidade, não oferecia grande segurança. De facto, a partir da época medieval começaram a utilizar-se técnicas de análise de frequência das letras na mensagem. Comparando a frequência das letras na mensagem transformada com a frequência média verificada em textos não transformados do mesmo idioma podia tentar-se identificar a regra de transformação que tinha sido utilizada.

No século XX foram introduzidas máquinas que já recorriam a operações matemáticas complexas para a transformação da mensagem. Ficou célebre a máquina Enigma, uma máquina eletromecânica inventada e utilizada pelas forças militares alemãs para comunicarem entre si, e que permitiu aos aliados, depois de descoberta a sua forma de funcionamento, intercetar as comunicações alemãs.

Desde então, a criptografia tem verificado significativos avanços, em particular desde o surgimento dos computadores digitais e, mais recentemente, pela aplicação de princípios da física quântica.

Neste capítulo daremos uma breve explicação das principais primitivas utilizadas em criptografia, isto é, os algoritmos criptográficos simples a partir dos quais é possível construir protocolos criptográficos avançados, como os utilizados na tecnologia Blockchain, e fundamentais para a compreensão do modo de funcionamento e da robustez desta tecnologia.

2.2 CONCEITO DE CIFRAGEM E DE ALGORITMO DE CIFRAGEM

Como dissemos, a criptografia preocupa-se em providenciar formas seguras de tornar uma mensagem inteligível por todos numa mensagem inteligível apenas por pessoas autorizadas.

Às mensagens ou textos inteligíveis por todos dá-se o nome de mensagem aberta ou texto aberto. Às mensagens ou textos inteligíveis apenas por pessoas autorizadas dá-se o nome de mensagem cifrada ou texto cifrado.

O texto diz-se cifrado porque é transformado num texto que apenas pode ser compreendido por quem disponha da cifra, ou segredo, para poder recuperar o texto original através de um processo de transformação inverso. Assim, a cifragem corresponde ao processo de transformação de um texto aberto num texto cifrado e a decifragem ao correspondente processo inverso.

Ao conjunto das operações executadas sobre o texto aberto para o transformar num texto cifrado dá-se o nome de algoritmo de cifragem (Figura 2.1).

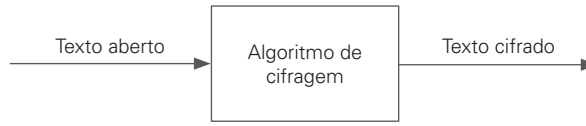


Figura 2.1 • Cifragem

O codificador de Atbash descrito na secção 2.1 é um exemplo de um algoritmo de cifragem. Com ele a mensagem "bom dia", inteligível por todos, é transformada na mensagem cifrada "yln wrz", apenas inteligível por quem tenha conhecimento de que, sobre a mensagem original, foi aplicado o codificador de Atbash.

2.3 O CONCEITO DE CHAVE CRIPTOGRÁFICA

No exemplo apresentado na secção 2.2, o algoritmo de cifragem apenas é sensível à mensagem a cifrar, a sua única variável de entrada, pelo que mensagens iguais produzem sempre mensagens cifradas iguais. Assim, basta conhecer as regras do algoritmo aplicado para ser possível recuperar a mensagem original a partir da mensagem cifrada (Figura 2.2).

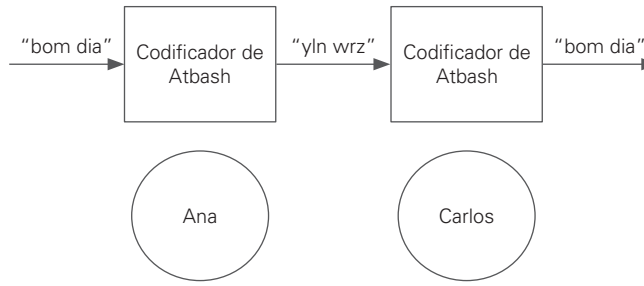


Figura 2.2 • Exemplo de cifragem/decifragem com o codificador de Atbash

DATA PROTECTION

A Blockchain tem o potencial de transformar profundamente organizações e sociedades. Ao permitir criar um novo tipo de sistema de registo (descentralizado, transparente, imutável e seguro, capaz de sincronizar uma visão comum do seu estado), emerge, da Blockchain, um protocolo de geração de confiança no sistema que dispensa, para o seu exercício, o recurso a entidades centrais.

A Blockchain permite, por isso, redesenhar cadeias de abastecimento, descentralizando, desintermediando, reduzindo custos e riscos, e assim incrementar a eficiência. O seu suporte a *smart contracts* (contratos digitais que autoexecutam as suas cláusulas) permite, também, a concretização de níveis sem precedentes de automatização dessas cadeias.

Este livro constitui uma primeira introdução à Blockchain, ao seu conceito, aplicabilidade e implicações. Começando por apresentar conceptualmente a Blockchain como um novo protocolo para geração de confiança, aborda seguidamente a rede Bitcoin e as criptomoedas. Avançando para a apresentação da rede Ethereum e do conceito de *smart contract*, aborda a evolução geracional para a Blockchain 2.0. Termina com uma reflexão sobre as implicações, não sem antes dar nota de casos reais de aplicação.

Destinado a gestores, decisores de TI/SI e ao público em geral.

TEMAS:

- **Confiança e geração de confiança**
- **Intermediação e descentralização**
- **Criptografia: confidencialidade, autenticidade e integridade**
- **Dinheiro: das *commodities* às criptomoedas**
- **Blockchain 1.0: bitcoin e ecossistema Bitcoin**
- **Blockchain 2.0: altcoins, *smart contracts* e Ethereum**
- **Exemplos de aplicação**
- **Implicações**

O primeiro livro escrito em Portugal sobre a Blockchain!
Uma obra que dá a conhecer os conceitos, as práticas e o futuro desta tecnologia, que vai muito além das criptomoedas. Com casos práticos de aplicação e uma previsão sobre as implicações da Blockchain na economia e na sociedade.

PEDRO MARTINS

Diretor de TI/SI no NOVO BANCO e Vice-Presidente da Associação Portuguesa de Data Science. Trabalhou para grandes multinacionais de consultoria, tendo executado variados projetos de TI/SI para diversas empresas financeiras, de telecomunicações e de energia.

ISBN 978-972-722-887-4

9 789727 228874

FCA

LIDEL

www.fca.pt