INSTITUTO POLITÉCNICO DE LISBOA
INSTITUTO SUPERIOR DE CONTABILIDADE
E ADMINISTRAÇÃO DE LISBOA

AUDITORIA FINANCEIRA DE BLOCKCHAIN: O ESTADO DA ARTE

Duarte Sala Lima

Lisboa, fevereiro de 2023

INSTITUTO POLITÉCNICO DE LISBOA
INSTITUTO SUPERIOR DE CONTABILIDADE E ADMINISTRAÇÃO DE LISBOA

AUDITORIA FINANCEIRA DE BLOCKCHAIN: O ESTADO DA ARTE

Duarte Sala Lima

Dissertação submetida ao Instituto Superior de Contabilidade e Administração de Lisboa para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Auditoria, realizada sobre a orientação científica do Professor Mestre Rui Manuel da Costa Vargas Pires, Professor Adjunto Convidado da área de Contabilidade e Auditoria.

Composição do Júri:

Presidente – Prof.a Doutora Paula Gomes dos Santos

Arguente – Prof. Especialista Pedro Roque

Vogal – Prof. Especialista Rui Manuel Vargas Pires

Lisboa, fevereiro de 2023

Dedicatória

A presente dissertação é dedicada a todos os intervenientes no processo da sua elaboração, quer direta quer indiretamente. Mais concretamente, e com um papel absolutamente primordial, dedico este trabalho à minha família que me é mais próxima, nomeadamente à minha irmã Matilde, à minha mãe Carla e ao meu pai João.

Agradecimentos

O resutado de um grande trabalho não advém de uma pessoa só, motivo pelo qual escrevo uma pequena mensagem a todos os que de uma forma ou de outra integraram a minha esfera social, profissional e académica.

Intrinsecamente relacionado com a elaboração da presente dissertação e com o meu percurso académico, agradeço em primeiro lugar ao Insituto Superior de Contabilidade e Administração de Lisboa, a instituição que me proporcionou a oportunidade de indagar uma temática deveras interessante e pertinente, a tecnologia Blockchain.

Um agradecimento obrigatório aos meus amigos que interviram de forma indireta no grande processo que é, e foi, a criação da presente dissertação. Mais concretamente, ao António Santos, ao Ricardo Carvalhal e ao Miguel Roque. As partilhas destes meus colegas de vida foram parte integrante do processo de escrita e exploração do universo da Blockchain.

Um especial e honesto agradecimento ao meu orientador e professor, tanto da Licenciatura como do Mestrado, Rui Vargas Pires, que cobriu toda a minha jornada académica e mais concretamente no desenvolvimento da presente dissertação.

"The whole world is a series of miracles,

but we're so used to them we call them ordinary things."

Hans Christian Andersen

Resumo

A presente dissertação procura estudar e enquadrar o atual contexto português de auditoria de Blockchain, tanto ao nível da literatura disponível à data, como na auscultação dos Revisores Oficiais de Contas (ROC) e da perceção destes relativamente a esta matéria.

Por forma a enquadrar teoricamente o tema, é explanado ao longo da dissertação os diversos desafios, benefícios e outras características da tecnologia Blockchain que se apresentam como potenciais transformadores da profissão e da forma como esta é exercida, quer ao nível dos principais riscos identificados e controlos que os mitiguem, como da validação das asserções através de procedimentos substantivos, permitindo ao auditor emitir uma opinião devidamente fundamentada.

Numa fase final do trabalho, serão validadas quatro hipóteses de estudo através de um questionário endereçado a todos os Revisores Oficiais de Contas. Após inferência dos dados recolhidos, é possível concluir que os mesmos consideram que a tecnologia Blockchain irá ter um impacto relevante na profissão de auditoria e na forma como os trabalhos de auditoria passarão a ser executados. Ainda afirmam que o seu nível de preparação para lidar com a tecnologia é bastante limitado e que as orientações emanadas pelos reguladores e pelas organizações profissionais, relacionadas com a tecnologia Blockchain, são insuficientes.

Palavras-chave: Blockchain, Riscos, Controlos, Procedimentos, Auditores Portugueses.

Abstract

This dissertation seeks to study and describe the current Portuguese context of Blockchain auditing, in terms of the literature available to date and the perception of the Certified Public Accountants regarding these matters.

In order to theoretically contextualize the theme, it is explained throughout the dissertation the various challenges, benefits and other characteristics of Blockchain technology that present themselves as potential transformers of the profession and the way it is exercised, both in terms of the main risks identified and controls that mitigate them, and the validation of assertions through substantive procedures, allowing the auditor to issue a properly grounded opinion.

In a final stage of the work, four study hypotheses will be validated through a questionnaire addressed to all Chartered Accountants. After inference from the collected data, it is possible to conclude that they consider that blockchain technology will have a relevant impact on the auditing profession and on the way audit work will be performed. They also state that their level of preparation to deal with the technology is very limited and that the guidelines issued by regulators and professional organizations, related to blockchain technology, are insufficient.

Keywords: Blockchain, Risks, Controls, Procedures, Portuguese Auditors.

Índice

Índice de Quadros

Índice de Tabelas

Índice de Figuras

Índice de Gráficos

Lista de Siglas e Acrónimos

AAA	American Accounting Association
AASB	Australian Accounting Standards Board
AD	Apresentação e Divulgação
AICPA	American Institute of Certified Public Accountants
AML	Anti Money Laundering
CMVM	Comissão do Mercado de Valores Mobiliários
CPA	Chartered Professional Accountants (Canada)
CPU	Central Processing Unit
EFRAG	European Financial Reporting Advisory Group
ERP	Enterprise Resource Planning
GITC	General IT Controls
IASB	International Accounting Standards Board
ICO	Initial Coin Offer
IEO	Initial Exchange Offering
IFRS	International Financial Reporting Standards
IFRS IC	International Financial Reporting Standards Interpretations Committee
ISA	International Standards on Auditing
ISAE	International Standard on Assurance Engagements
KYC	Know Your Costumer
OROC	Ordem dos Revisores Oficiais de Contas
OS	Organização de Serviços
PCAOB	Public Company Accounting Oversight Board
POA	Proof of Authority
POS	Proof of Stake
POW	Proof of Work
ROC	Revisor Oficial de Contas
SOC	Service Organization Controls
STO	Security Token Offering
TI	Tecnologias de Informação

1. Introdução

A Blockchain apresenta-se como uma tecnologia disruptiva e potencialmente transformadora de muitas indústrias, desde os serviços financeiros às instituições públicas, prometendo reformular o sistema económico e financeiro tal como é conhecido. Estando a mesma associada à segurança e validação de dados em transações, a Auditoria não lhe passará ao lado, quer seja através da sua aplicação em criptomoedas, ou outros ativos digitais como contratos ou até mesmo informações pessoais.

Neste sentido, aplicar os métodos tradicionais de auditaria a criptoativos[1] suportados pela tecnologia Blockchain apresenta-se como desadequado e incapaz de transmitir ao auditor uma segurança razoável na avaliação dos riscos, na validação das asserções e, consequentemente, na formulação da opinião a emitir.

A elaboração da presente investigação tem como um dos dois objetivos, sintetizar e preencher as lacunas existentes na literatura produzida aos dias de hoje quanto à tecnologia Blockchain e à sua aplicação à Auditoria. Embora organismos profissionais como a American Accounting Association (AAA) e a Chartered Professional Accountants do Canadá (CPA), as grandes auditoras e alguns trabalhos académicos já se tenham debruçado sobre esta temática, é possível constatar a ausência de uma análise abrangente que proporcione aos auditores, aos reguladores e a outros interessados, uma compilação do "estado da arte" da auditoria a entidades em que a tecnologia Blockchain tem um impacto relevante nos seus processos de relato financeiro e/ou nas suas operações.

Assim, o trabalho inicia-se com uma introdução das características técnicas da tecnologia Blockchain, seguindo-se do aprofundamento da importância da auditoria de blockchain tal como das considerações que o auditor deve seguir numa auditoria financeira em ambiente de Blockchain.

Complementarmente, a presente dissertação tem como segundo objetivo aferir qual o sentimento dominante no seio da profissão em Portugal, via auscultação dos Revisores Oficiais de Contas, relativamente a: (i) impactos que a tecnologia Blockchain irá ter ao nível da profissão de auditoria; (ii) impactos que a tecnologia Blockchain irá ter ao nível dos trabalhos de auditoria; (iii) nível de preparação dos ROC para lidar com esta tecnologia no

[1] Note-se que, para efeitos de dissertação, a menção a "criptoativos" corresponderá a criptoativos e/ou a criptopassivos, correspondendo, assim, à informação inscrita numa blockchain.

âmbito dos seus trabalhos; (iv) nível de apoio que os ROC têm sentido da parte dos reguladores e das organizações profissionais em lidar com esta tecnologia no âmbito dos seus trabalhos. A aferição desta realidade será efetuada tendo por base a realização de um inquérito junto destes profissionais. No âmbito deste processo serão ainda validadas as seguintes hipóteses de trabalho:

a) É convicção dos ROC que a tecnologia Blockchain irá ter um impacto relevante na profissão de auditoria (H1). Esta hipótese é suportada por Brender e Gauthier (2018), Leoni e Schmitz (2019) e Bible, Raphael, Riviello e Taylor, (2017);
b) É convicção dos ROC que a tecnologia Blockchain irá ter um impacto relevante na forma como os trabalhos de auditoria passarão a ser executados (H2). Esta hipótese é suportada por Catalini e Gans (2017), Boulianne, E., Clark, J., Eskandari, S. e Pimentel, E. (2021) e Dai e Vasarhelyi (2017);
c) É convicção dos ROC que o seu nível de preparação para lidar com a tecnologia Blockchain é bastante limitado (H3). Esta hipótese é suportada por Gambhir (2018) e por Forbes (2019);
d) É entendimento dos ROC que as orientações emanadas pelos reguladores e pelas organizações profissionais, relacionadas com a tecnologia Blockchain, são insuficientes (H4). Esta hipótese é suportada por Charbonneau (2020) e por Abreu, Aparício e Costa (2018).

O trabalho que me proponho realizar consiste na investigação destes impactos, culminando na apresentação das principais vantagens e dificuldades impostas pela Blockchain no âmbito da auditoria de demonstrações financeiras materialmente influenciadas por esta tecnologia.

2. Os Ativos Digitais e a Blockchain

Os ativos digitais correspondem a registos eletrónicos que por sua vez correspondem a direitos ou obrigações com reconhecimento nas demonstrações financeiras. Este tipo de ativos (ou passivos) está representado em "livros de registos" que não correspondem necessariamente a uma blockchain. Ou seja, todos os ativos inseridos numa blockchain correspondem a ativos digitais, mas nem todos os ativos digitais estão suportados por uma blockchain. O presente capítulo, tal como a dissertação como um todo, pretendem retratar o "estado da arte" destes dois conceitos recentemente inseridos na profissão de auditoria. Mais concretamente, este capítulo procura introduzir, numa primeira instância, o conceito e a utilidade dos ativos digitais e, numa segunda instância, desenvolver o conceito da tecnologia Blockchain, enquanto um conceito técnico, por forma a facilitar o enquadramento aos capítulos seguintes.

2.1. Os Ativos Digitais

A Deloitte, no seu Global Blockchain Survey de 2020, define Digital Assets como "something represented in a digital form that has intrinsic or acquired value". Ao qual acrescento que estes ativos são representados, suportados e transacionados numa blockchain ou numa tecnologia semelhante. As criptomoedas correspondem aos primeiros tipos de criptoativos criados, no entanto já se pode contar com representações digitais de terrenos, *commodities*, moeda fiduciária, dívida ou capital "tokenizados", instrumentos financeiros, e muito mais.

Como analogia, pode-se afirmar que os tokens correspondem a uma moeda, como uma "ficha" de casino ou para comprar bebidas numa discoteca. Há diversas categorias de tokens, sendo as principais: (1) tokens de acesso, onde é desenvolvido um serviço que requer a utilização dos seus próprios tokens (como o exemplo da "ficha" nos casinos); (2) tokens de suporte, onde o emissor do token afirma possuir reserva de valor sendo que o token representa o direito de reclamar esse valor; (3) tokens de capital, onde uma empresa emite tokens que representam as partes do capital próprio.

Enquanto atualmente a esmagadora maioria das transações são registadas em softwares e ERP, como por exemplo o SAP, a mesma transação pode ser registada numa blockchain. As

blockchains além das comuns transações, ainda podem registar a troca de bens físicos e de criptoativos entre as partes.

Quando o termo criptoativo (ou criptopassivo) é utilizado, referimo-nos a ativos e passivos registados nos balanços das empresas e que são transacionados utilizando a tecnologia Blockchain.

Os criptoativos são criados através da criptografia (técnica de comunicação segura e escrita em código informático) que define a quantidade disponível, a finalidade e a forma como as transações são registadas. As transações de criptoativos são muitas vezes armazenadas e validadas em blockchains de acesso público, pelo que este tipo de ativos corresponde a reservas de valor e a meios de troca como é o caso das moedas digitais (criptomoedas) ou os tokens digitais que permitem o acesso a produtos e serviços das empresas (Bennett *et al*., 2020).

No estudo suprarreferido da Deloitte, em que são inquiridos 1.488 *senior executives* e profissionais distribuídos por 14 localizações, é indicado que 83% dos inquiridos dizem que acreditam fortemente, ou de alguma forma, que os ativos digitais irão servir como uma alternativa, ou substituir, a atual moeda fiduciária nos próximos 5 a 10 anos. Na China continental esta percentagem ascende a 94%.

Os ativos digitais vêm proporcionar a "tokenização" dos ativos físicos, permitindo que a troca dos mesmos seja mais facilitada e com menos restrições gerando ainda um alto nível histórico de transparência e de registo das transações.

O estudo da Deloitte ainda refere que quase 90% dos inquiridos acreditam que os ativos digitais irão ser muito, ou de alguma forma, importantes para as suas indústrias nos próximos três anos.

Aos dias de hoje, a emergência sucessiva de criptoativos já trouxe a atenção de todo o tipo de *stakeholders*, incluindo entidades normalizadoras, profissionais dos diversos mercados, reguladores, políticos e académicos.

Já no Deloitte's 2021 Globlal Blockchain Survey, é indicado que as barreiras regulatórias e a cibersegurança correspondem aos maiores obstáculos de aceitação dos ativos digitais. O mesmo estudo ainda afirma que a tecnologia Blockchain está na vanguarda da mudança de todo o sistema financeiro, desde a aceitação de depósitos, aos pagamentos, empréstimos, investimentos e comércio de qualquer coisa que tenha valor.

Estes criptoativos também conseguem ser alternativas para a dívida clássica ou angariação de financiamento, através de métodos de angariação de capital como, por exemplo, Initial Coin Offerings (ICO), Security Token Offerings (STO) ou Inicial Exchange Offerings (IEO), que recorrem à emissão de criptoativos e já reuniram cerca de 31,1 mil milhões de dólares até setembro de 2019, como enunciado pelo 6th ICO / STO Report: A Strategic Perspective. Spring 2020 Edition da PwC.

Os ativos digitais e os criptoativos já tomaram a atenção dos bancos centrais. O Banco de Portugal (2021) publicou um vídeo explicativo, intitulado de "O que são os criptoativos?", em que indica que está a ser equacionada, um pouco por todo o mundo, a emissão de uma moeda digital dos respetivos bancos centrais (no caso da zona Euro, o Banco Central Europeu com o "euro digital"), garantindo assim um meio de pagamento confiável e sem custos, que viria completar, mas nunca substituir, o numerário. O projeto ainda está em fase de investigação e ao longo dos próximos anos o Eurosistema ainda vai analisar como é que o "euro digital" poderá ser concebido e distribuído de forma a satisfazer as necessidades dos cidadãos europeus, de modo que o Euro continue a ser um símbolo de progresso e merecedor da confiança dos cidadãos europeus.

2.2. A Blockchain

Após a revolução da internet no século XX, está a emergir, nos dias que decorrem, "o valor da internet", que consiste em coisas como o dinheiro, ações e obrigações, propriedade intelectual (música e arte), o voto e até a nossa entidade, que podem ser enviadas para o outro lado do mundo em segurança e instantaneamente, sem um intermediário.

Foi David Chaum, criptógrafo, que em 1982, através da publicação da sua dissertação, apresentou a primeira proposta de algo semelhante a uma blockchain - cadeia de informação agrupada em blocos na internet. Mais tarde, em 1991, Stuart Haber e W. Scott, também criptógrafos, procuravam implementar um sistema onde a informação aí introduzida jamais pudesse ser adulterada (Golaszewski, Javani, Sherman & Zhang, 2019).

Anos mais tarde, em 2008, surge Satoshi Nakamoto, com a criação da primeira blockchain. Esta blockchain foi específica e unicamente desenvolvida para a Bitcoin, correspondendo assim à tecnologia que tornou possível a existência desta criptomoeda.

A Blockchain é uma tecnologia distribuída e descentralizada de registo eletrónico de dados. Isto é, distribuída porque todos os utilizadores têm acesso a 100% da informação e descentralizada porque não existe uma entidade central que a controla.

Uma base de dados tradicional é criada por uma autoridade central que a controla e decide quem tem acesso e que informações armazenam e arquivam. Este tipo de base de dados apresenta algumas desvantagens, isto é, caso a autoridade central esteja comprometida ou se se estiver na presença de uma fuga de informação (exposição ou invasão de *hackers*), a base de dados apresenta-se vulnerável e em risco. O poder centralizado permite que o controlo seja limitado a um reduzido número de pessoas, traduzindo-se, na maioria dos casos, num controlo humano sobre as informações de uma transação. Por exemplo, na contratação de um crédito bancário, apesar da grande maioria dos procedimentos poderem ser efetuados online, ainda é necessário a validação de assinaturas e de outros aspetos contratuais por parte de humanos, o que leva a que o processamento da transação seja oneroso, moroso, vulnerável a *hackers*, limitado às pessoas que a operacionalizam, requer *skills* especiais e está sujeito à ocorrência de erros humanos. Neste sentido, a tecnologia Blockchain resolve todos estes desafios, afirma o professor do Massachusetts Institute of Technology (2020), Gary Gensler.

A Deloitte (2019) define que as blockchains são "protocols that allow entities to store and share transactional information in a controlled and systematic way". Já o Banco de Portugal, num vídeo de explicativo intitulado de "O que são os criptoativos?", indica que uma blockchain consiste em

> blocos [de informação] ligados entre si por ordem cronológica, [incluindo] uma componente de criptografia e fórmulas matemáticas que garantem que a informação guardada não pode ser adulterada. É a tecnologia que habitualmente está na base dos criptoativos.

A Blockchain é um novo tipo de base de dados, que por ser descentralizada, está disponível para qualquer utilizador ter acesso, ao mesmo tempo que garante a imutabilidade da informação. Contudo, qualquer criptógrafo pode criar uma blockchain, o que leva a que apesar da Blockchain permitir a descentralização dos dados, a tecnologia pode ser empregue em sistemas centralizados como forma de assegurar a integridade dos dados e dos utilizadores e, ao mesmo tempo, reduzir os custos operacionais de uma organização.

As funcionalidades inerentes a uma blockchain, derivam das seguintes características intrínsecas que uma blockchain pode ter[2]:

- Imutável – os dados inseridos na Blockchain não podem ser alterados ou apagados;
- Em tempo real – registo de transações quase em tempo real;
- Ambiente de confiança – registo das transações entre as partes sem a necessidade de um terceiro que proporcione confiança;
- Distribuída – rede de registos distribuídos e de acesso público;
- Compensatório – promove a validação correta da informação através de atribuição de recompensas a quem executa a validação;
- Auditável – o historial das transações é acessível a quem pretenda rever os acontecimentos ocorridos na rede.

2.3. Como Funciona uma Blockchain?

A Blockchain é uma tecnologia que, com base em criptografia[3], permite guardar, validar e autorizar transações digitais. Uma blockchain corresponde a uma cadeia de dados armazenados em blocos. Cada bloco é, como descrito por Freire (2021), composto por: "um aglomerado de informação (*data*), um identificador do bloco (*hash*) e um *hash* associado ao bloco imediatamente anterior na cadeia. Neste sentido, os *hashes* correspondem ao elemento de ligação entre os blocos, como exemplificado na Figura 2.1.

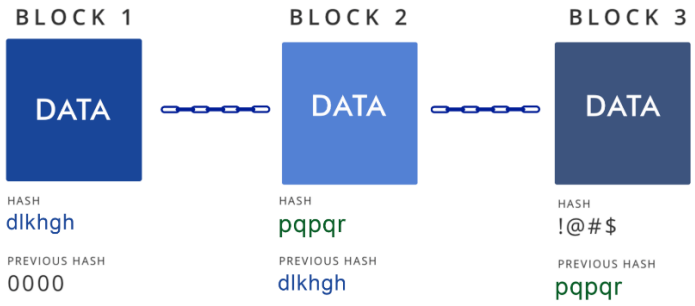


Figura 2.1 Ilustração de uma cadeia de blocos.

Fonte Blog "blockchainexpert".

[2] Dependerá de como a blockchain for construída, isto é, do seu protocolo, mecanismo de consensos, etc.
[3] A criptografia tem como principal objetivo permitir duas pessoas comunicarem de forma segura num canal de informação, impedindo a interferência de terceiros na sua mensagem. É uma ciência que procura encriptar a informação por meio de código que só pode ser descodificado por quem estiver na posse da chave de desencriptação.

Cada bloco tem um único *hash* que identifica a transação - também conhecido como a "impressão digital" da transação. Quando se utiliza a *private key*[4] para assinar a mensagem, está-se a produzir um "*hash*" que consegue ser verificado com a *public key*[4] (Boulianne *et al*., 2021).

É de notar que daqui em diante, e devido às inúmeras variantes que esta tecnologia pode ter, considera-se na presente dissertação a generalização da Blockchain como uma base de registo eletrónico de dados distribuída e descentralizada.

Uma blockchain armazena informação em blocos que se ligam entre si numa ordem cronológica. A adição de novos blocos individuais representa o aumento do histórico das transações ocorridas nessa base de dados, esclarece Nofer, M., Gomber, P., Hinz, O. e Schiereck, O. (2017). Os blocos são validados (confirmados) pela rede de *miners*[5], através da criptografia, e enviados para os *nodes*[6] de forma a garantir que a rede está em consenso, ou seja, que toda a informação é verdadeira. No caso da Bitcoin a base de dados utilizada corresponde à sua própria blockchain.

Em suma, como é que isto acontece? Para se perceber a ciência por detrás desta tecnologia, é necessário compreender os grandes conceitos que, ao se interligarem, permitem a existência de um "livro de registos" acessível a qualquer ser humano e controlado por nenhum: (i) o protocolo, ou as "regras do jogo", (ii) os participantes (inclui *miners* e utilizadores[7]), quem e de que forma participa na rede e (iii) a validação dos blocos, validação da informação gerada pelo consenso dos participantes.

De uma forma resumida, a interligação destes conceitos e o funcionamento de uma blockchain pode ser simplificada da seguinte forma: alguém cria uma blockchain definindo as regras com que a blockchain se autogovernará (o protocolo), sendo que posteriormente quem quiser participar poderá fazê-lo através da utilização "normal" da blockchain

[4] A *public key* (chave pública na sua tradução literal) corresponde ao típico "*username*" (para identificação) em oposição à *private key* (chave privada na sua tradução literal) que corresponde à típica "*password*" (para assinar as operações realizadas). Ambas as *keys* fazem parte da criptografia implementada em qualquer blockchain.

[5] Os *miners* (mineiros na sua tradução literal) são indivíduos que validam e aglomeram as transações em blocos e, posteriormente, adicionam-nos à rede de blocos existentes (blockchain). Os *miners*, além da validação da informação, também têm como função a criação de novos blocos que por sua vez podem gerar novas unidades de Bitcoin, por exemplo.

[6] Os *nodes* (nó ou nódulos numa tradução literal), são pequenos computadores capacitados para armazenar toda a informação relacionada com as transações ocorridas numa blockchain.

[7] Termo utilizado apenas para efeitos da dissertação.

(participantes) e/ou através da examinação da informação que é introduzida pelos participantes "normais" (participantes e a validação dos blocos).

2.3.1. O Protocolo

O protocolo é definido pelo seu criador, através de uma linguagem de programação, que consiste na definição das regras que permitem a blockchain operar como pretendido. Estas regras são imutáveis[8] após a conceção da plataforma, traduzindo-se assim na descentralização da mesma.

O protocolo define as características da blockchain, nomeadamente, a descentralização e a distribuição da mesma. Ou seja, o criador da blockchain pode optar por desenhar uma blockchain privada e definir quem a controla e quais são os utilizadores que têm acesso, mantendo outras características e utilidades fundamentais de uma blockchain, como é o caso da imutabilidade. Por outro lado, as regras definidas pelo criador no protocolo podem passar por criar uma blockchain de acesso público - descentralizado e distribuído. Em qualquer um dos casos, no protocolo estará definido o mecanismo de obtenção de consensos (onde se inclui a atividade dos *miners* e a respetiva recompensa) e quem pode participar – aspetos a analisar nos pontos seguintes.

É a partir do protocolo, e de como este foi desenhado que se pode concluir, em certa parte, quanto à segurança dos dados proporcionada pela blockchain em questão.

2.3.2. Os Participantes

Para efeitos da dissertação, considera-se que os participantes numa blockchain se podem dividir em dois grupos: (1) os *miners* (operam os *nodes*), que mantêm a blockchain a funcionar como se se tratasse de uma equipa de manutenção – e (2) os utilizadores, que utilizam e acedem ao serviço proporcionado pela blockchain. Sem a atividade dos primeiros, os últimos não conseguiam executar operações numa blockchain.

Pode-se dizer que uma blockchain existe nos *nodes*, ou seja, uma blockchain corresponde a um conjunto de *nodes* que estão interligados entre si (*online*) e constantemente a comunicar uns com os outros por forma a que a informação contida nestes esteja sempre atualizada. Um

[8] Se houver consenso da maioria da rede para redefinir as regras, as mesmas podem ser alteradas, no entanto apenas se for consensual (pelo menos 51%). Tem-se o exemplo da blockchain do Ethereum, que alterou o mecanismo de consensos de *proof of work* para *proof of stake*, modificando assim o seu protocolo.

node corresponde a um equipamento informático, como um computador, um *smartphone* ou um *tablet*, que tem uma cópia da blockchain armazenada e que vai sendo atualizada com os novos blocos. Só para a blockchain da Bitcoin é estimado que existam milhares de *nodes* ativos (ligados à *internet* e a atualizar o registo de transações de bitcoins). Qualquer indivíduo pode ter um *node* a funcionar, o que pode significar a possibilidade de existência de milhões de cópias atualizadas da informação de uma blockchain.

São os *nodes* que armazenam, partilham e preservam a blockchain. Existem diversos tipos de *nodes* que têm diversas funções e que podem coexistir em simultâneo ou não - depende sempre das características (do protocolo) da blockchain em causa. Os diferentes tipos de *nodes* podem contribuir de diferentes formas para a rede, contributos esses que podem ser: verificar a validade da informação e dos blocos, transmitir os diversos blocos pelos restantes *nodes* da rede, proteger a blockchain e garantir que as regras definidas pelo protocolo estão a ser seguidas e outros ainda podem contribuir para a celeridade e privacidade de transações.

Na presente dissertação não serão abordados os diferentes tipos de *nodes* existentes, mas considera-se importante mencionar um dos tipos de *nodes* essenciais ao funcionamento de uma blockchain: os *full nodes*. Estes mantêm uma cópia de todo o histórico de informação na blockchain (pode atingir *terabytes* de informação, o que se traduz num grande dispêndio e capacidade de armazenamento, mas adiciona resiliência[9] à rede porque, mesmo que um *full node* desapareça, a informação mantém-se devido à partilha online da informação entre os restantes *nodes*) e validam os novos blocos na rede[10]. É a rede que irá chegar a um consenso sobre aceitar o novo bloco na blockchain.

À semelhança dos *nodes*, qualquer indivíduo ou entidade coletiva pode ser um utilizador na blockchain, desde que o protocolo subjacente tenha definido esta blockchain como aberta ao público. Se for privada (centralizada), é necessário obter autorização.

Um utilizador corresponde a alguém que pretende executar transações ou guardar informação[11] numa blockchain, para fins profissionais ou pessoais. A estes é-lhes atribuído

[9] Quantos mais *full nodes* participarem numa blockchain, mais segura esta se torna. Em teoria, apenas é necessário um *full node* para que a rede funcione, porém mais suscetível a ataques informáticos quando comparado com a tentativa de adulterar milhares de cópias.

[10] Sem a cópia integral da blockchain, não seria possível os *nodes* validarem as novas transações e blocos. Exemplo com bitcoins: se não se sabe qual o atual saldo das partes que intervêm na transação (para saber o saldo necessito do histórico da atividade desses mesmos intervenientes), não haverá possibilidade de saber se a parte que paga tinha bitcoins suficientes para efetuar o pagamento.

[11] A informação pode corresponder a qualquer coisa, como por exemplo os direitos de um retrato artístico, de uma música, de uma imagem ou de um vídeo.

uma *private key* e uma *public key* que serve de meio para interagir com a blockchain. O utilizador é assim proprietário de uma *address wallet*[12] na qual pode armazenar o seu histórico de informação. A *public key* corresponde ao típico "*username*" (para identificação) em oposição à *private key* que corresponde à típica "*password*" (para assinar as operações realizadas). Ambas as *keys* fazem parte da criptografia implementada em qualquer blockchain.

Como indicado por Freire (2021), a criptografia é aplicada da seguinte forma: "[a] mensagem é encriptada quando um utilizador envia uma mensagem para outro utilizador (para a public key deste). A partir daqui só o utilizador que tenha a chave privada correspondente pode ler a mensagem."

2.3.3. A Validação dos Blocos

Os blocos ligados entre si pelo *hash* (cada bloco é identificado com o seu *hash* e com o *hash* do bloco anterior, e assim sucessivamente) contêm a informação que é inserida na blockchain, transação após transação. É o facto de os blocos estarem ligados estre si, que permite que haja uma sequência lógica, temporal e segura. Isto permite que só haja uma sequência possível e que permanecerá para a história dos registos da blockchain, não podendo sofrer alterações.

Para isto acontecer, os participantes concordam com o protocolo (mais concretamente, com o mecanismo de consensos), em que cada novo bloco de transações é examinado e validado. Se um potencial novo bloco está em conformidade com o protocolo, é considerado como verdadeiro (existe consenso) e é inserido no "livro de registos", a blockchain, ou seja, é distribuído por toda a rede de *nodes* (a informação deste novo bloco é adicionada às cópias da blockchain existentes em todo o mundo).

O conceito que se considera chave é o mecanismo de consensos. Este exige que, com base no definido pelo protocolo, haja uma uniformização e coerência dos dados que são validados e assumidos como verdadeiros por todos os *nodes*. Caso contrário, está-se perante cópias diferentes da blockchain e esta deixa de ser descentralizada e distribuída – assume-se que a blockchain está desprotegida, ou seja, inexistência de consenso entre os participantes.

[12] Uma *address wallet* (morada da carteira na sua tradução literal) corresponde ao endereço criado para se poder transacionar e inserir informação na blockchain, como se se tratasse de uma conta bancária num banco.

O perigo da ausência de consenso está no controlo indevido da blockchain (monopolização do *mining*[13] em pelo menos 51%) que pode levar ao *double-spending*[14]. Como afirmado por Sayeed e Marco-Gisbert (2019), quem controlar 51% do *mining* consegue efetuar as seguintes ações dentro da blockchain: "double-spend the same crypto-coin, restrict transactions, cancel blocks, and even have full control over the price of a cryptocurrency". O que o controlador nunca conseguirá fazer é criar transações em nome de outros participantes porque seria necessário a respetiva *private key*, constata Freire (2021).

É de notar que existem diversos tipos de blockchain que podem ser construídas o que implica diferentes protocolos. Isto leva a que a monopolização do *mining* em 51% e o *double-spending* apenas possam ocorrer em determinados protocolos. Existem outros métodos de deturpar uma blockchain, no entanto a presente dissertação centrar-se-á nos conceitos gerais proporcionados pela tecnologia Blockchain.

Existem vários mecanismos de consenso que podem ser utilizados pelas blockchains. De seguida debruçamo-nos sobre os principais, mas distintos, mecanismos de consenso: o *proof of work* e o *proof of stake*.

2.3.3.1. Proof of Work

O *proof of work* (doravante denominado de POW) é um mecanismo de obtenção de consensos que se baseia na resolução de uma equação matemática. É o mecanismo de consensos mais utilizado atualmente, sendo inicialmente utilizado pela Bitcoin, e rapidamente implementado por outras grandes blockchains. Os *miners* são o grande pilar do mecanismo de consensos POW e do processo de autorização e registo das transações aprovadas pelos mesmos, como indicado por Sayeed e Marco-Gisbert (2019).

No POW, a informação é agregada e registada na blockchain através do *mining* de blocos, protegendo a mesma contra eventuais ataques, pois, como indica Freire (2021), para os executar, seria necessário grande poder computacional e tempo para fazer os cálculos envolvidos no trabalho de *mining*. Os custos gerados pelo ataque ultrapassariam a possível recompensa, diminuindo a motivação que seria necessária para um *miner* executar um ataque nocivo.

[13] O *mining* (mineração na sua tradução literal) corresponde à atividade exercida pelos *miners.*
[14] O *double-spending* (gasto duplo na sua tradução literal) consiste no gasto de uma unidade de criptomoeda e, posteriormente, adulterar a rede por forma a que volte a gastar a mesma moeda mas noutra transação.

Relativamente à segurança da informação armazenada numa blockchain, o criador da Bitcoin (Sakamoto, 2008) afirma que "[t]he system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes", o que na prática se traduz numa probabilidade extremamente reduzida da rede ser penetrada.

Isto porque, ainda Sakamoto (2008), a blockchain é representada por uma "maioria decisiva" (em que cada *node* corresponde a um "voto", sendo que os *nodes* são controlados/possuídos pelos *miners*), que corresponde a um determinado CPU *power*[15]. Para um *hacker* levar a cabo a adulteração de um bloco, seria necessário refazer o trabalho previamente efetuado nesse bloco, e em todos os blocos seguintes, por forma a ultrapassar o trabalho dos "*honest nodes*"[16]. Probabilidade essa que foi refutada matematicamente pelo autor na sua publicação, afirmando que a mesma reduziria cada vez mais à medida que seriam adicionados novos blocos, ou seja, à medida que o tempo vai passando.

Neste sentido, são transferidos incentivos para os *miners* como forma de remuneração, pois são eles que garantem a segurança da blockchain, , como explicado por Nakamoto (2008),

> The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins.

A Deloitte, na sua investigação sobre Blockchain em 2018 (Deloitte, 2018), cita Nolan Bauerle ao dizer que a Blockchain é

> the particular orchestration of three technologies (the Internet, private key cryptography, and a protocol governing incentivization)" that resulted in a secure system for digital interactions without the need for a trusted third party to facilitate digital relationships.

Em suma, seria necessário o *hacker* controlar e alterar pelo menos 51% das dezenas de milhares de cópias[17] da blockchain espalhadas por todo o mundo em *nodes* ativos.

As desvantagens do POW resumem-se aos elevados custos de computação e ao facto de depender bastante de energia elétrica. O *mining* da Bitcoin consumiu cerca de 10,95 TWh

[15] Poder computacional gerado na agregação dos *nodes*.
[16] *Nodes* que contribuem para o normal funcionamento e crescimento da rede.
[17] No caso da Bitcoin são dezenas de milhares, em outras blockchains podem ser mais ou menos, consoante o número de *nodes* ativos nessa blockchain.

no mês de janeiro de 2022[18], que extrapolado para um ano completo, corresponde a cerca de 131 TWh, superando o consumo da Argentina no ano de 2019, um país com cerca de 44 milhões de habitantes. Ou seja, com base nos consumos apresentados para a Bitcoin, um *miner* nocivo necessitaria de consumir cerca de pelo menos metade da eletricidade consumida pela Argentina para poder adulterar a blockchain da Bitcoin, pois esta baseia-se em POW.

Por forma a compreender melhor o trabalho executado pelo mecanismo de consensos POW, é necessário clarificar o que é o *mining* e como funciona. Numa primeira abordagem é necessário indicar que são os *miners* que executam o processo de *mining*.

Quando os utilizadores querem que determinada informação fique registada numa blockchain, eles enviam-na aos *miners*. Conforme Freire (2019), os *miners*

> recebem e verificam a informação. Posto isto, se esta estiver conforme (ou seja, se a informação respeitar as regras do protocolo) o/os miner/s juntam-na à memory pool, que é como que um espaço de gestão temporária de memória, onde a informação fica armazenada até os miners a incluírem no seu próximo bloco. Depois agregam a informação retirada da memory pool num bloco.

O processo de *mining* de um bloco é detalhado como descrito de seguida. Inicia-se com o *hashing* das transações enviadas pelos utilizadores aos *miners* e, como indicado por Freire (2019)

> esses hashes são organizados em merkle trees ou hashing trees, que não são mais do que a organização de hashes em pares para serem consequentemente hashed até que se alcance o último hash também chamado root hash ou merkle root.

Os elementos de "identificação" de um bloco, como exemplificado na Figura 2.2, são: o *hash* gerado para o próprio bloco, o *hash* do bloco anterior e um *nonce* (número aleatório). Estes elementos correspondem ao cabeçalho do bloco que, como esclarecido por Freire (2019),

[18] Cf. University of Cambridge – Judge Business School: Cambridge Centre for Alternative Finance, disponível em: https://ccaf.io/cbeci/index.

> é depois *hashed* produzindo um output (*hash*) que identificará o bloco e deverá começar com "x" zeros consecutivos consoante a dificuldade do *mining*. Quando este é encontrado, o *miner* transmite o bloco pelos [*nodes*] que verificam se o *hash* é valido e se for adicionam o bloco à sua cópia da blockchain.

Este *hash* é a prova do trabalho, ou seja, o POW dos *miners*.

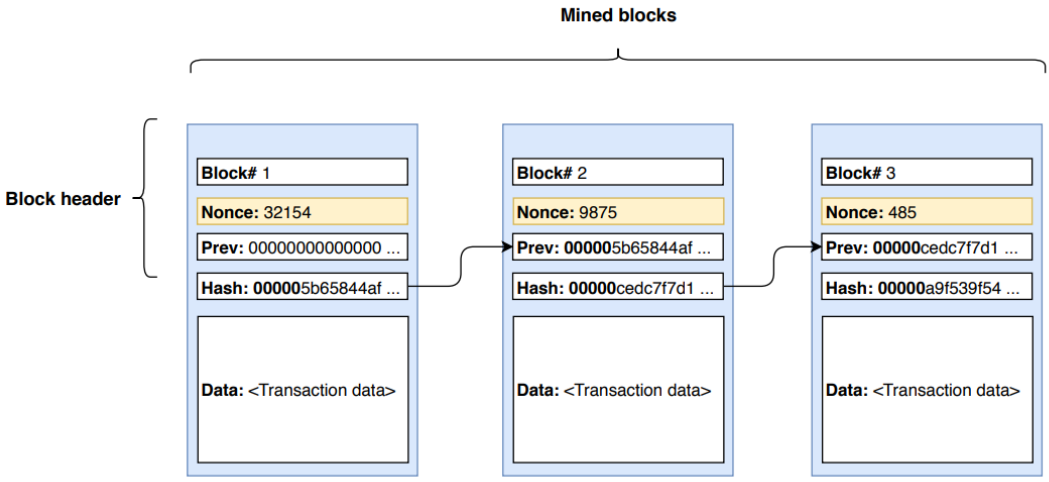


Figura 2.2 Ilustração do processo de *hashing* desde o genesis block.
Fonte Ali *et al.* (2019).

No caso de um *miner* encontrar um *hash* válido ao mesmo tempo que outro *miner*, para o mesmo bloco, cada um irá transmitir o seu bloco para a rede. Este acontecimento gera uma ramificação temporária (*fork*) que irá fazer com que existam duas versões do histórico, o que permite efetuar o *double-spending*. Uns *miners* irão receber um bloco e outros irão receber o outro bloco. Daqui em diante eles irão trabalhar com o *hash* do bloco anterior que receberam. "Este problema é solucionado através da presunção do protocolo que a Blockchain mais comprida é a verdadeira" explica Freire (2019). O autor continua, com referência a Nakamoto (2008)

> [q]uando isto acontecer, uma ramificação da cadeia ficará maior que a outra. Então os utilizadores que tinham a cópia da Blockchain que se tornou mais curta irão trocar esta cópia pela que agora é mais comprida[19].

[19] Diversas corretoras esperam por seis confirmações do bloco em causa antes de executar as transações nele contidas, afirma Sayeed e Marco-Gisbert (2019).

Na Figura 2.3 verifica-se que foram distribuídos para a rede blockchain, praticamente ao mesmo tempo, dois blocos diferentes (A e B). Quando isto acontece, espera-se para identificar qual é que é a versão correta da blockchain. A versão correta será a que se estender mais. Probabilisticamente, um deles continuará mais do que o outro e ganhará – ou seja, é deveras improvável que duas versões diferentes de uma mesma blockchain continuem lado a lado ao mesmo tempo.

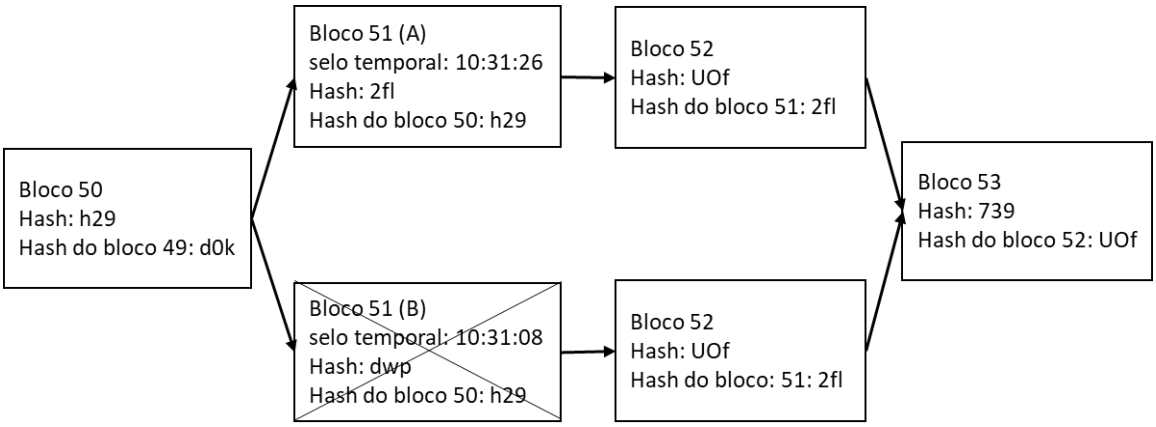


Figura 2.3 Ilustração da criação e da resolução de um fork.

Fonte Freire (2021).

Em termos rigorosos, não é a maior cadeia de blocos que irá ser escolhida pelos *nodes* como a versão correta mas sim a que que tiver mais provas dadas de trabalho executado (maior quantidade de *hash power*). Será o bloco da cadeia de blocos que apresentar o maior *hash power*, que a rede (*nodes*) irá assumir como a versão verdadeira da blockchain. O bloco que ficar "só" (versão mais curta) deixará de ser considerado na versão verdadeira e as transações nele contidas, que sejam verdadeiras, já se encontravam na versão verdadeira da cadeia de blocos (caso contrário não seria a versão verdadeira).

Os *nodes* diferem dos *miners* no sentido em que os primeiros aceitam nas suas versões da blockchain os blocos que são validados pelos segundos. A professora do Massachusetts Institute of Technology (2019), Neah Narula, explica que, cada *node* (individualmente) lê a informação dos novos blocos validados pelos *miners* e procedem à sua aceitação ou rejeição, tendo como base os parâmetros (regras) definidos no protocolo. Um *node* nunca aceitará uma transação inválida mesmo que esta esteja incorporada numa versão com mais *hash power*. Relativamente ao *mining* de Bitcoin, Ahmed et al. (2018), afirmam que no algoritmo de POW,

> miners try their best to solve a cryptographic puzzle by calculating the hash of a block header twice with the SHA-256 function. Solving this puzzle is referred to as Bitcoin mining.

Do POW resulta que, quanto mais poder computacional for utilizado para validar os blocos, mais segura é a blockchain. Redes mais pequenas e com um mecanismo de consensos de POW menos ativo, apresentam um nível de vulnerabilidade maior, visto um *miner* malicioso necessitar de menos poder computacional para penetrar a rede.

O *hashing* – geração de um *output* (*hash*) através de um *input* (informação a armazenar na blockchain) – corresponde a um processo, que aliado à criptografia, torna a informação armazenada na blockchain mais segura pois exige um elevado dispêndio de recursos. Os *outputs* (que no caso da blockchain da Bitcoin correspondem a uma sequência de 64 letras e números aleatórios) são gerados pelos algoritmos de *hashing*[20] tendo como base a informação armazenada. Como exemplificado no Quadro 2.1, basta apenas a informação a armazenar (*input*) alterar uma letra de minúscula para maiúscula, para que o *output* gerado seja aleatoriamente alterado. Este exemplo de geração de outputs é universal e corresponde ao algoritmo SHA-256, o algoritmo utilizado pela Bitcoin.

Quadro 2.1 Outputs gerados pelo algoritmo SHA-256 para a palavra "auditoria"

Input	***Output* (*hash*)**
Auditoria	3C7D69019FF37F53BE07EF597A99E043E E776F6C537B7458377094C0919D1CD6
AUDITORIA	D99F95EBB121716C4E1B06B131552D98 FB32E3934FA1F8E3D59282F0676D89E5
auditoria	1645A130998FAD9863020B28848CCC23 F95861CD7A63C4C4C0A89E175159E144

Fonte Utilizado um website para executar a simulação. Disponível em: https://codebeautify.org/sha256-hash-generator.

[20] Existem diferentes algoritmos de *hashing*. Como enunciado por Freire (2019): "[e]xistem o SHA-0, SHA-1, SHA-2 e SHA-3. O algoritmo utilizado pela Bitcoin é o SHA-256, que é um modelo do SHA-2. Atualmente considera-se que apenas o SHA-2 e SHA-3 são seguros, uma vez que nos SHA-0 e SHA-1 já se descobriram colisões." Por colisões pode-se entender como sendo um factor de insegurança da informação, conceito que não irá ser abordado na presente dissertação.

A importância dos algoritmos de *hashing* assenta no facto de que, para o *input* armazenado (imagine-se que a informação que se pretende guardar na blockchain era a palavra "Auditoria") só irá haver um único possível *output*, e é através desse output e do facto de a ligação entre cada bloco necessitar do output do próprio bloco e do output do bloco anterior, que se robustece a segurança de uma blockchain. Isto porque em qualquer momento aquela informação introduzida gerará sempre o mesmo output e todos os outputs da blockchain encontram-se interligados, um a um, protegendo a integridade dos dados. A alteração dos dados originais fará com que os utilizadores rejeitem essa alteração, visto a mesma não estar concordante com a restante blockchain

Na Figura 2.4 pode-se verificar uma os dados originais de uma blockchain.

Figura 2.4 Ilustração de uma blockchain.
Fonte Freire (2021).

Na Figura 2.5 pode-se verificar os dados da mesma blockchain mencionada Figura 2.4, mas que neste caso foi corrompida.

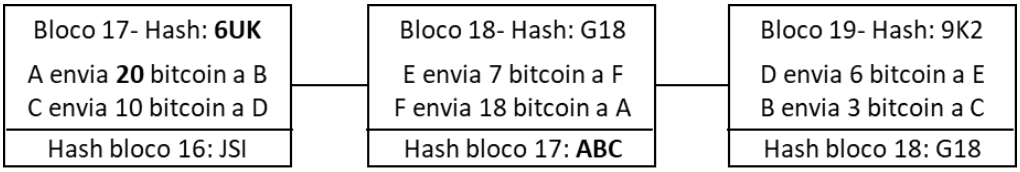


Figura 2.5 Ilustração da blockchain constante da Figura 2.4, mas que foi corrompida.
Fonte Freire (2021).

Os milhares de *nodes* que validam a informação e armazenam as cópias da blockchain, ao identificarem que a blockchain foi corrompida, rejeitam essa alteração e mantêm a versão original da cópia. Um *miner* corrupto, perante uma tentativa de alteração da blockchain, "só terá uma opção e esta traduz-se em fazer o *mining* de todos os blocos subsequentes até encontrar um *hash* válido para todos eles", afirma Freire (2019). Fazer o *mining* de todos os blocos seguintes significa, como visto anteriormente, possuir a maioria do poder computacional (*hash power*), energia (eletricidade) e de tempo para fazer os cálculos envolvidos no trabalho de *mining*.

Daqui se tira que para um *miner* corrupto executar o seu objetivo, será necessário ele adicionar blocos mais rapidamente que o resto da rede, o que implicaria que o *miner* corrupto estivesse na posse de mais poder computacional do que os restantes *miners* da rede inteira que trabalham em conjunto para a versão verdadeira da blockchain. Ou seja, a prova de trabalho que prevalece corresponde à que investir mais recursos.

2.3.3.2. Proof of Stake

Proof of stake (doravante designado por POS) "is a consensus mechanism which authorizes blocks based on the stakes a participant pours into the network", indica Sayeed & Marco-Gisbert (2019). Em oposição ao POW, que recorre à utilização da energia e de poder computacional, o algoritmo POS elege um participante para validar o próximo bloco com base na combinação de alguns requisitos definidos no protocolo. Estes requisitos consistem, numa primeira abordagem, na percentagem de participação (*stake*) da criptomoeda utilizada na blockchain que o participante tem na rede. Ou seja, "quanto maior for a *stake* do participante, maior será a probabilidade de ser selecionado para forjar um bloco", indica Freire (2019). Quem valida terá que bloquear uma certa quantidade de criptomoeda na blockchain como prova de intenção (POS), o que constitui um mecanismo de segurança, visto diminuir a probabilidade de alguém querer controlar a rede, pois perderia aquelas criptomoedas bloqueadas.

A segunda abordagem deste mecanismo de consenso consiste em colmatar o potencial favorecimento dos maiores detentores da criptomoeda da blockchain. Para isso, existem diversas soluções possíveis que ajudam ao não enviesamento do processo de seleção. Os processos de seleção mais utilizados são o *randomised block selection* (seleção aleatória) e o *coin age selection* (seleção com base na antiguidade que o *miner* detém a criptomoeda).

A recompensa para quem cria blocos, no mecanismo de consensos POS, passa por taxas de transação, ou seja, o autor da transação pode incrementar a recompensa do *miner* por forma a que este dê prioridade à validação dessa mesma transação. No seu artigo, Ciaian (2021) indica que no caso da remuneração de um *miner* de um mecanismo de consensos de POW, o prémio deste consiste na oportunidade de validar o bloco e com isso ser remunerado com um montante de criptomoeda previamente determinado.

No fundo a Blockchain é um sistema que fornece um registo permanente de valor – transações, eventos, contratos, ativos, identidades, etc. – dentro de uma comunidade sem que

haja a necessidade de uma reconciliação manual e de um controlo central. A validação das transações é efetuada por indivíduos aleatórios dispersos pelo mundo, cujo fator em comum é o fato de todos trabalharem para um único mesmo objetivo.

2.4. O Exemplo do Ethereum e dos *Smart Contracts*

A Bitcoin é uma rede descentralizada de pagamentos, conforme indicado por Martins (2018), que utiliza bitcoins como moeda de transação e utiliza a tecnologia Blockchain para operar a rede e registar os pagamentos. A rede ao ser descentralizada permite reduzir os custos de transação – consequência da eliminação de intermediários. Neste momento, as bitcoins são consideradas por muitos investidores como uma representação digital de valor e/ou reserva de valor – também conhecidas por muitos investidores como o "*digital gold*" (Gore, 2020).

Em 2014 foi criada a Ethereum que corresponde a uma plataforma de Blockchain que possibilita múltiplas aplicações[21] como registos eleitorais, financeiros e médicos e executar uma grande variedade de contratos - os *smart contracts*. Os benefícios de passar estas aplicações para redes de blockchain, prendem-se com os principais atributos e características de uma blockchain, como a descentralização, a distribuição, a imutabilidade e a segurança.

Adiciona-se que o Ethereum também tem uma criptomoeda em circulação – Ether – que funciona como moeda de troca nas operações efetuadas no seio desta blockchain. Posto isto, verifica-se que a blockchain da Ethereum tem uma aplicação muito superior à da blockchain da Bitcoin.

Note-se que, a presente dissertação está a utilizar o Ethereum como exemplo, no entanto salvaguarda-se que também foram criadas outras blockchains com características iguais ou semelhantes. Tudo depende das características do protocolo e do nível de criptografia programados pelo seu criador.

2.4.1. O Ethereum

O Ethereum baseia-se na tecnologia Blockchain tal como a bitcoin. No entanto é completamente diferente porque está desenhada para suportar mais aplicações quando comparada com a da bitcoin, que apenas foi desenha para fazer face às transações da criptomoeda. Tem, assim, um propósito múltiplo ao invés de um propósito único. Isto porque

[21] Ver subcapítulo 2.5 para mais aprofundamento das aplicações da tecnologia Blockchain.

suporta escritas criptográficas distintas, enquanto a blockchain da Bitcoin apenas suporta uma programação criptográfica.

Esta plataforma de *software* usa a Blockchain e os *smart contracts* para permitir a construção de complexas aplicações de *software* descentralizadas, tendo em vista a criação de soluções que não requerem a tradicional cadeia de comandos hierárquicos e sendo aplicações que não têm um único indivíduo que obriga a projetar as regras.

O criador do Ethereum está a aprimorar a sua blockchain de modo que, devido à dimensão e volume de transações, possa globalizar-se e tornar a sua blockchain aplicável às mais distintas utilidades possíveis. Ao invés de todas as transações serem validadas por todos os *miners*, cada um destes apenas validaria uma parte aleatória dos movimentos ocorridos na blockchain.

Em suma, Ethereum 2.0 foi uma atualização ocorrida em 2022, que centrou-se na alteração do mecanismo de consensos de POW para POS e, posteriormente, atualizar o *Sharding*. O *Sharding* resolve os problemas de escalabilidade, pois, em suma, ao invés de cada *miner* da rede necessitar de fazer o *download* de todas as transações e validar todas as transações, eles apenas necessitariam de fazer o *download* e de validar uma porção das transações, num sistema aleatório. Por exemplo, substitui-se dez *miners* validarem mil transações, por cinco *miners* validarem mil transações e os restantes cinco *miners* validarem outras mil transações. Deste modo, o Sharding permite aumentar o número de transações por segundo, visto cada computador individualmente manter o mesmo número de validações, enquanto no agregado as validações aumentarem, ao mesmo tempo que reduz o custo destas validações.

2.4.2. Os *Smart Contracts*

Os *smart contracts* podem ser comparados a uma *vending machine* que é programada para executar uma ação caso se verifiquem as condições previamente definidas e acordadas. Podem ser utilizados em seguros e contratos financeiros, por exemplo.

Projetos de angariação de capital, onde se define que, se os utilizadores enviarem o dinheiro suficiente para a blockchain no período definido, o dinheiro vai para quem procura angariar capital, caso contrário volta para os indivíduos que queriam investir no projeto. Há inúmeras regras que podem ser desenvolvidas em código, o que se traduz em inúmeras possibilidades e variedades de tipos de *smart contracts*.

Por exemplo, um fotógrafo que detém a propriedade de uma fotografia e que a quer vender, pode criar um *smart contract* que irá permitir, em certas condições por este definidas, a venda da mesma, sendo executada a transação e entregue uma cópia da fotografia ao comprador. A transação é guardada na blockchain para sempre como prova do que aconteceu. Acrescento que o detentor original pode, por exemplo, obter um *royaltie* sobre cada venda subsequente da obra que criou e introduziu na blockchain.

Outra situação de um *smart contract* é quando duas partes utilizam um *smart contract* na contratação de um derivado de cobertura do preço do *brent* à data do fim do período. Quando os termos do contrato estiverem estabelecidos, estes ficam anexados à blockchain juntamente com os fundos apostados (cativação dos fundos). No fim do período, o *smart contract* irá ler o preço do *brent* através de uma referência de confiança definida no *smart contract* (conhecido como "*oracle*"), calcular o montante acordado e transferir os fundos diretamente para a *address wallet* da parte beneficiária.

Uma desvantagem dos *smart contracts* reside no facto de, no caso de erros, não ser possível voltar atrás, perdendo por exemplo os tokens ou deixar um *bug* (erro na redação do contrato) que permite a utilização indevida do token/contrato. Porém, os problemas com a execução de contratos, o número de procedimentos legais e o risco de fraude proveniente do aumento da transparência podem ser reduzidos com a implementação de soluções como os *smart contracts*.

2.5. Aplicações Práticas da Blockchain

A utilização de blockchains para armazenar informação de uma forma segura e permanente apresenta inúmeras aplicações à realidade, quer no seio dos mercados financeiros, investimentos e instituições financeiras, quer nos múltiplos tipos de indústrias que existem espalhadas pelo mundo. As vantagens associadas à sua utilização diferem de entidade para entidade e de organização para organização. No presente subcapítulo podemos encontrar um breve resumo das suas vantagens e de algumas possíveis aplicações práticas que o mercado se encontra a desenvolver.

2.5.1. Vantagens da Utilização de Blockchain

Face às características intrínsecas de uma blockchain, podemos salientar diversas vantagens associadas à sua utilização. Começando pela regulação, e tendo em consideração a

descentralização de uma blockchain, pode-se afirmar que a informação armazenada numa blockchain não se encontra sujeita a uma regulação específica de uma nação ou espaço geográfico, visto a mesma estar disponível a qualquer parte que apresente meios e recursos para aceder à *internet*. No caso de blockchains privadas, pode-se afirmar que qualquer utilizador autorizado a aceder a essas blockchains poderá, em qualquer parte do mundo, aceder à informação nelas contida.

Através de uma blockchain também se pode afirmar estar perante uma redução de custos operacionais dada a oportunidade de anular, parcial ou totalmente, processos repetitivos, morosos, manuais e suscetíveis de erro.

Outra praticabilidade encontrada na tecnologia Blockchain é a redução do tempo de contratualização, desde o momento em que se indica que se pretende "fechar" um contrato até ao momento em que o contrato é efetivamente "fechado" com a receção do dinheiro, por exemplo. Este período pode ser encurtado devido ao facto de, por exemplo, o dinheiro poder ser enviado entre continentes em segundos, contrastando com os tradicionais dias ou semanas. A redução significativa das taxas de serviço que são pagas corresponde a outra vantagem.

A segurança e a privacidade dos intervenientes das operações efetuadas numa blockchain consiste em mais uma grande vantagem intrínseca da tecnologia. Os utilizadores estão identificados com *public keys* ao invés dos seus nomes próprios como comummente acontece.

2.5.2. Casos de Uso e Aplicações da Blockchain

A Blockchain está cada vez mais a ser aplicada em diversas finalidades, dada a capacidade de suporte e apoio ao desenvolvimento dos negócios, estando mais e mais organizações inseridas num processo de aprendizagem dos benefícios oferecidos por esta tecnologia emergente. É de salientar que a primeira utilização prática começou com o armazenamento dos primeiros registos de transações da criptomoeda Bitcoin, mas que as perspetivas futuras de aplicação são ilimitadas e dependem apenas da imaginação do Homem.

O valor acrescentado que uma blockchain pode proporcionar aos negócios é múltiplo, sendo enunciados de seguida alguns exemplos: transparência – todos os participantes conseguem visualizar os novos dados inseridos; confiança – não é necessário os participantes conhecerem-se para que confiem na informação; desintermediação – a confiança elemina a

tradicional necessidade de um intermediário para gerar confiança; permite *smart contracts* – estes contratos só são passíveis de serem desenvolvidos, trocados e executados em sistemas de Blockchain; auditável – os registos são imutáveis, datados e eternos, o que os torna auditáveis.

Nos parágrafos que se seguem são enunciados exemplos de setores de negócio onde a tecnologia se apresenta como emergente e com visíveis vantagens aplicacionais.

Como enunciado pela Forbes (2019), relativamente aos investimentos, no mercado financeiro, o uso da Blockchain tem potencial de provocar grandes transformações. Com a tecnologia, será muito mais fácil "fracionar" e transacionar as frações de um ativo, desde ações de empresas até uma propriedade imobiliária, o que, consequentemente, proporciona mais liquidez, reduz os custos por transação e alavanca a universalidade do acesso a diversos ativos. Outra aplicabilidade nesta área está relacionada com as transações globais desses ativos, que poderiam ser feitas por pessoas em qualquer lugar do mundo. Ou seja, para o mercado de investimentos, a Blockchain pode representar uma injeção de liquidez e a universalização de acesso para negociações de diversos ativos.

Na saúde, ao termos em conta uma das características da Blockchain, a rede distribuída de registo de dados, esse fator resolveria um problema bastante comum nesta área: a gestão de registos médicos. Dificilmente os pacientes têm o controlo de acesso ao histórico de saúde numa base única, passando a ser detentores da informação – exames, apontamentos médicos e receitas geralmente estão espalhados nos diversos sistemas de informação dos prestadores de serviços do paciente ou até mesmo em arquivos físicos. Com o uso da Blockchain, todo esse conjunto de dados poderia ser compilado num único lugar, facilitando o acesso e, principalmente, proporcionando ao paciente o direito de usar os dados de acordo com os seus critérios, em situações em que isso possa contribuir para um aumento da assertividade dos tratamentos.

O conceito emergente da Internet das Coisas (IoT) também representa um caso de possível aplicação da tecnologia. Aqui a Blockchain possibilita a criação de sistemas de micropagamentos entre dispositivos, o que permitiria a estes dispositivos realizar tarefas em benefício da rede e serem "remunerados" por isso. Noutras palavras, seria possível um frigorífico gerar informações sobre o ambiente em que se encontra, informando um termostato se deve ou não ligar o ar-condicionado. Esse mesmo termostato pode entrar em

contacto com a central mais próxima dos bombeiros caso detete um potencial incêndio. Isto tudo automaticamente.

No negócio da agricultura, o principal benefício seria a transparência e a procedência das *commodities*. O histórico completo de um determinado tipo de grão, por exemplo, pode ser rastreado com o uso da blockchain, possibilitando ao comprador saber a origem, qualidade e condições de armazenamento.

Como nem tudo são rosas na tecnologia Blockchain, já existem questões levantadas por diversos autores no que diz respeito à confiança no sistema. Apontando como uma das maiores vantagens da Blockchain, a confiança que é gerada ao serem eliminados diversos intermediários inerentes a uma cadeia de processos, Bennet *et al.* (2020) salientam que a Blockchain não funciona sozinha e que esta é alimentada por fontes de informação externas. Ou seja, apesar dos elevados níveis de integridade da informação gerada pela Blockchain, os autores levantam desafios relativamente à qualidade da informação que é introduzida na Blockchain. O exemplo real da IBM Food Trust é explorado pelos referidos autores. Neste caso, a blockchain permite aos fornecedores, retalhistas e consumidores monitorizarem em tempo real o percurso de bens alimentares desde que são colhidos até alcançarem o consumidor final. Neste exemplo os produtos contaminados conseguem ser localizados na cadeia de abastecimento e eliminar a fonte da contaminação. Apesar da imutabilidade das informações fornecidas pela Blockchain, "they do not address the risk that suppliers upload unverified information to the blockchain. Academics have referred to this as the "first-mile problem"", afirmam os autores. No caso da blockchain construída pela IBM, o problema encontra-se na possibilidade de os agricultores introduzirem informação incorreta na blockchain.

Os mesmos autores ainda relatam o mesmo problema quando aplicado em sistemas de relato financeiro. É de entendimento geral dos pioneiros da Blockchain que, quando esta tecnologia for combinada com a inteligência artificial, estar-se-á perante uma automatização de diversos processos financeiros, como o preenchimento de contratos, pagamentos e recebimentos e até do preenchimento de declarações fiscais. Perante esta automatização, que exige um armazenamento volumoso de informação, os autores questionam: "how do we know that the information on blockchains that contribute to financial reporting systems is reliable?"

Os autores exemplificam este problema com o preenchimento de um contrato. Utilizando um contrato que se executa automaticamente (*smart contract*), têm-se que: a entrega dos bens ocorre após os termos do contrato serem satisfeitos, incluindo o pagamento e o recebimento. Relacionando a automação dos contratos com o trabalho dos auditores, os autores afirmam

> [i]t is evident to me that auditors will still need to ensure that the smart contract is a legitimate contract with legitimate parties for legitimate goods and consideration. Hamm (2018), a member of the U.S. audit regulator the PCAOB, articulated this point in a speech: "Blockchain does not magically make information contained within it inherently trustworthy.

Em suma, apesar das possíveis mudanças provocadas pela Blockchain e pela inteligência artificial, o papel dos auditores permanecerá importante na certificação da qualidade das operações financeiras das entidades.

Ainda se pode considerar que as áreas de aplicação da Blockchain são extensíveis às entidades estatais e às atividades que outro tipo de organizações executam. É o caso das organizações de caridade que têm frequentemente um programa de angariação de fundos para, por exemplo, países de terceiro mundo, o que implica envio de fundos para localizações muito distantes. Aqui tem-se outro exemplo onde a Blockchain permite efetuar transferências monetárias com baixo custo burocrático e com maior transparência no que concerne às regulações de branqueamento de capitais.

Também tem-se que, os produtos digitais, sem o suporte de uma blockchain, têm sido bastante fáceis de mover entre dispositivos pelo que também os torna muito fáceis de serem copiados ou roubados, como é o caso dos artistas de música que perderam milhares de milhões de euros porque é difícil provar a validade da detenção de um produto digital. Por exemplo, se um fotógrafo profissional guardasse a fotografia numa blockchain, seria difícil alguém tentar ficar com os créditos dessa mesma fotografia, dado o registo de propriedade ficar guardado na blockchain e ser extremamente improvável alguém alterar esse facto.

Também se pode analisar o exemplo real das transportadoras logísticas da Maersk e a IBM que, em conjunto, estão a iniciar a utilização de Blockchain nas transações dos portos reduzindo imenso o número de autorizações necessárias para cada produto (até 30 pessoas), ao que se junta o facto de diminuir a exposição ao risco de fraude ou roubo.

Através do já referido estudo da Deloitte (2021) sobre a Blockchain, é possível concluir que, atualmente, as utilizações mais frequentes da tecnologia Blockchain nas organizações correspondem à troca de informação segura e ao armazenamento e transações de moedas digitais.

Portanto, neste sentido, a Blockchain corresponde a uma tecnologia que oferece características – autonomia, descentralização, segurança e transparência - que são normalmente providenciadas por terceiros como os notários, intermediários financeiros internacionais ou auditores.

2.6. A Evolução da Blockchain

A primeira blockchain foi implementada há 14 anos. Nessa altura, de acordo com o Deloitte's 2020 Global Blockchain Survey, esta tecnologia apenas estava perspetivada como uma mera plataforma de pagamentos de criptomoeda. Com o passar dos anos, a plataforma passou para algo verdadeiramente disruptivo, o que se confirmou com o aumentar dos investimentos realizados.

Das sondagens sobre Blockchain efetuadas pela Deloitte, de 2019 para 2020, verificou-se uma transformação de opinião e posição face à Blockchain, passando de dúvidas e incertezas a parte integrante de estratégias adotadas por empresas e organizações dos diversos setores.

As organizações, atualmente, estão mais comprometidas com a Blockchain porque, à medida que o tempo passa, elas estão a introduzir e implementar esta tecnologia no seu dia-a-dia. Ou seja, uma das conclusões desta pesquisa é que os líderes já não consideram a inovação como promissora, mas sim como algo de concreto, palpável e como parte da sua organização.

Neste sentido, e com base nas sondagens da Deloitte (2018, 2019 e 2020), podemos observar que os respondentes que achavam que a Blockchain ia ser crítica e que seria incluída no top 5 de prioridades estratégicas da empresa, passaram de 43% em 2018, para 53% em 2019, para 55% em 2020.

Paralelamente à tendência anterior apresentada, a Tabela 2.1 indica outros tópicos.

Tabela 2.1 Resultados dos inquéritos da Deloitte sobre Blockchain

Questão	2018	2019	2020
A tecnologia Blockchain é escalável e irá atingir uma adoção generalizada	84%	86%	88%
A nossa equipa executiva acredita que há utilidade da tecnologia Blockchain para o nosso negócio	74%	83%	86%
A minha organização ou projeto irá perder vantage competitiva se não adotar a tecnologia Blockchain	68%	77%	83%

Fonte Deloitte's 2018, 2019 e 2020 Global Blockchain Survey.

A empregabilidade de colaboradores com perícia em Blockchain também se destaca com 82% dos inquiridos a afirmar em 2020 que estão ou vão contratar pessoas com estas qualificações, face aos 73% em 2019.

Conclui-se que a tendência da adoção da Blockchain passou de "turismo" para uma exploração de aplicações práticas auxiliares aos negócios, como afirma o referido estudo da Deloitte (2020). Mais especificamente, são os serviços financeiros e as *fintech* (setor das empresas tecnológicas financeiras) os líderes nos desenvolvimentos da Blockchain. Refuta-se esta conclusão com o facto de em 2020, 39% dos inquiridos afirmarem que já têm aplicações de Blockchain no ativo, face aos 23% em 2019.

3. Enquadramento Geral de Relato Financeiro

Como resultado de uma tecnologia emergente, subsistem atualmente diversas dúvidas relacionadas com o relato financeiro de criptoativos (e de criptopassivos). De facto, parece haver um consenso alargado nos meios profissional e académico de que as normas de relato financeiro atualmente em vigor, em particular as Normas Internacionais de Relato Financeiro (IFRS), são insuficientes para assegurar um tratamento abrangente e coerente desta temática.

Em algumas jurisdições os respetivos organismos de normalização optaram por proporcionar orientações específicas relativamente a alguns criptoativos, em particular relativamente a

criptomoedas. O IFRS IC (Comité de Interpretações das IFRS) pronunciou-se igualmente sobre esta tipologia de criptoativos. Persistem, porém, muitas lacunas e dúvidas que urge esclarecer.

A estrutura conceptual do International Accounting Standards Board (IASB), atualizada em 2018, que define um ativo como um recurso económico presente (direito suscetível de gerar benefícios económicos futuros) controlado pela empresa em resultado de acontecimentos passados, permite considerar os criptoativos como ativos visto conseguirem satisfazer todas as condições atrás elencadas. Porém, podem surgir dúvidas quanto ao registo dos mesmos devido à opacidade e incerteza da posse dos direitos associados aos criptoativos (insuficiente documentação e acordos contratuais, exemplo: cerca de 80% das ICO eram esquemas, indica o European Financial Reporting Advisory Group (EFRAG), 2020).

Entre 2016 e 2018, 1.300 milhões de USD de criptoativos foram roubados, tipicamente devido à obtenção fraudulenta (através de ataques de hackers, por exemplo) da private key ou devido a erros de programação. No entanto, estes ataques não devem impedir que seja efetuado o reconhecimento do ativo como explicado pelo EFRAG (2020).

O Reino Unido já considera, através de enquadramento legal específico, a possibilidade de os criptoativos serem considerados como propriedade e permite que os smart contracts sejam legalmente aceites, o que contraria a posição de alguns *stakeholders* que consideram que os criptoativos não se enquadram na lei (EFRAG, 2020).

O IFRS IC clarificou que, no espectro do normativo atual, as criptomoedas enquadram-se na Norma Internacional de Contabilidade (IAS) 2 – Inventários quando são detidas para venda no decurso ordinário do negócio (à semelhança dos requisitos do parágrafo 3 (b) da IAS 2 para commodities), sendo, neste caso, mensuradas pelo seu justo valor deduzido dos custos para vender. Quando a finalidade da sua detenção for distinta, devem ser considerados como ativos intangíveis de acordo com a IAS 38 – Intangíveis. Conclui também que não podem ser considerados como dinheiro nem como um outro ativo financeiro (IAS 32), na medida em que não constituem um meio de troca nem uma unidade de medida, não constituem um investimento em instrumentos de capital próprio de outra entidade, não têm associado um direito contratual de receber dinheiro ou outro ativo financeiro ou de trocar ativos ou passivos financeiros e não são um contrato que seja ou possa ser liquidado através de instrumentos de capital próprio do detentor.

Estas considerações do IASB são consistentes com as da Australian Accounting Standards Board (AASB) e do Chartered Professional Accountants of Canada (CPA Canadá).

Embora este entendimento expresso pelo IFRS IC proporcione orientações úteis para o relato financeiro de criptoativos, o seu alcance parece ser insuficiente, atendendo à multiplicidade de tipologias de critpoativos e de criptopassivos que existem e que vão muito para além do fenómeno das criptomoedas.

Há questões e desafios relacionados com esta temática que urge responder e clarificar, sendo de destacar os seguintes:

- Esta natureza de ativos e passivos é distinta de todas as outras especificamente tratadas nas normas de relato financeiro em vigor, ou faz sentido tratar estes ativos e passivos como sendo de naturezas específicas?
- Poderão alguns destes ativos e passivos enquadrar-se em tipologias já adequadamente tratadas pelas normas em vigor, ao passo que outros são distintos e, consequentemente, requerem a criação de normas específicas para dar resposta aos mesmos?
- Desafios no reconhecimento e mensuração de criptoativos (e de criptopassivos), tais como:
    - Abordagens de mensuração que reflitam os reais atributos destes ativos e passivos;
    - Identificação de mercados ativos e de técnicas de mensuração de justo valor na ausência de tais mercados;
    - Adequação da definição de caixa e equivalentes de caixa à finalidade e utilização de alguns destes criptoativos;
    - A multiplicidade de formatos, utilizações e enquadramentos legais de *utility/hybrid tokens*;
    - Considerações específicas para a detenção de criptoativos em nome de outros;
    - Questões que derivam das características específicas das plataformas DLT usadas.

Por exemplo, atendendo a estes desafios, o EFRAG (2020) remete para uma publicação do AASB (2016) que sugeria a criação de uma segunda norma relacionada com ativos

intangíveis com finalidades de investimento, à semelhança do que já sucede com os ativos fixos tangíveis (com a distinção das propriedades de investimento).

Existem, assim, mais questões do que respostas relativamente ao relato financeiro de criptoativos (e de criptopassivos), sendo esta um área que carece de atenção especial urgente.

4. A Importância da Auditoria de Blockchain

De acordo com Wolfson (2020), Henri Arslanian, o líder global de criptomoedas da PwC, afirmou em entrevista à Cointelegraph que as "*Big Four*" representam um papel muito importante no desenvolvimento do ecossistema das criptomoedas, ao referir

> Although Bitcoin was designed with a trustless ideology, the reality is that the industry still requires trusted entities to catalyze the development of the ecosystem.

A auditoria fornece confiança, a todos os *stakeholders*, de que as empresas estão a operar de forma transparente e a aderir aos *standards* setoriais. Neste sentido, com o crescimento e maturação dos negócios dos ativos digitais e as legislações e regulamentações a tornarem-se mais robustas, os auditores continuam a desempenhar um papel fundamental.

A implementação da tecnologia Blockchain levará o seu tempo. No entanto, Gambhir (2018) afirma que quando este sistema de registos de informação tornar a consulta de transações fácil e generalizada, as empresas e os auditores irão aderir à tecnologia. Afirma ainda: "the way businesses are audited will clearly change, as will the responsibilities and agendas of the audit committee."

Apesar das blockchains oferecerem transparência total do histórico das transações, os auditores ainda têm um papel fundamental. De acordo com Leopold (2020), posteriormente à penetração das blockchains nos *business processes*, ainda se verificará a necessidade de avaliar o risco de fraude ou erro, tal como a avaliação dos controlos gerais informáticos. Como o autor indica: "[h]aving access to realtime information from a blockchain opens new opportunities for real-time assurance and more timely reporting."

Interpretando as Normas Internacionais de Auditoria (ISA), verifica-se que o auditor deve desenhar e executar procedimentos de auditoria cuja natureza, tempestividade e extensão dependem e dão resposta aos riscos de distorção material identificados ao nível das asserções. Dado os criptoativos não serem ativos tangíveis e, por natureza, apenas

"existirem" em formato digital na Blockchain, os procedimentos de auditoria tipicamente requerem o uso de informação obtida (ou derivada) de uma blockchain pública – por forma a servirem de evidência de auditoria que irá mitigar os riscos identificados, mesmo em ambientes de Blockchain.

A Forbes (2019), em parceria com a KPMG, desenvolveu um estudo sobre a importância dos conhecimentos de Blockchain nos profissionais de auditoria. Concluiu-se que 79% (dos 250 executivos de finanças inquiridos) têm a expectativa de que os seus auditores proporcionem entendimentos relativamente ao impacto da Blockchain nos seus negócios ou no relato financeiro.

Em suma, o papel do auditor e da presença da auditoria no ambiente empresarial perspetiva-se como fundamental e permanecerá como um garante de fiabilidade das demonstrações financeiras das entidades, com possibilidade de se extender a outros trabalhos de garantia de fiabilidade.

4.1. O Auditor vs A Blockchain

O papel da Blockchain tem sido visto por muitos como uma fonte de verificação de informação em que são os *miners* quem valida as transações. No entanto, a verificação e validação providenciada pela Blockchain (são os *nodes* que validam a informação) opõem-se à verificação fornecida pelos auditores das demonstrações financeiras.

Analisando as perspetivas em dois prismas diferentes, tem-se que por um lado a informação contida numa blockchain pode ser considerada como irrefutável (Crosby, Kalyanaraman, Nachiappan, Pattanayak & Verma, 2016) e beneficiar de "*costless verification*" (Catalini & Gans, 2017) e, por outro lado, o facto da Blockchain não verificar se a informação introduzida está em concordância com os normativos de relato financeiro ou se é legítima. Ou seja, a Blockchain verifica se a transação ocorreu, a correspondente data e o respetivo montante, mas não proporciona, por exemplo, uma análise dos controlos internos, subjacentes ao processo de relato financeiro, que previna ou detete erros e fraude, como proporcionado por uma auditoria às demonstrações financeiras. Neste sentido, será necessária a intervenção do auditor para a validação da informação que alimenta a blockchain.

Na perspetiva de Boulianne *et al.* (2021), a atividade da auditoria não pode ser substituída por uma blockchain, porque é muito mais do que a verificação de transações rotineiras. Trata-se da verificação da robustez dos controlos internos da empresa, das suas políticas de relato e da razoabilidade de estimativas significativas.

No processamento de um registo contabilístico de uma transação, as entidades devem procurar ir ao encontro e respeitar os normativos legais e de relato financeiro. O mesmo aplica-se ao registo de uma operação contabilística numa blockchain. Nestes casos, ambas as partes chegam a acordo relativamente às condições subjacentes à transação (quais os bens a trocar, valor de troca, data de troca, etc.), e quando chega a hora da execução da transação, a mesma é registada numa blockchain. Apesar de ambas as partes conseguirem aceder à composição da transação, validando a ocorrência, os montantes e o corte das operações, as mesmas, além de poderem estar a incumprir (por fraude ou erro) com os seus normativos contabilísticos e legais, também desconhecem se a contraparte está a cumprir com os normativos desta. Ou seja, não é por ambas as partes de uma transação aceitarem e executarem as condições subjacentes a uma transação que essas condições estão conforme as leis, normativos e regulamentos a aplicar.

É nestas situações que o auditor desempenha um papel fundamental por forma a garantir a fiabilidade da informação financeira. Assim, descarta-se a hipótese de que a tecnologia Blockchain não irá substituir o trabalho do auditor, pois ambos revelam-se como componentes importantes e insubstituíveis na produção de informação financeira de qualidade.

4.2. Impacto da Blockchain na Auditoria

A inclusão da Blockchain nos processos, nos controlos internos, nos sistemas de informação e como tecnologia subjacente a ativos ou passivos das entidades leva a que os auditores procurem novas respostas na avaliação e na resposta aos riscos de distorções materialmente relevantes das demonstrações financeiras de negócios e entidades que adotem esta tecnologia. Assim, emerge a necessidade da criação de novas abordagens de auditoria que mitiguem os riscos subjacentes e assegurem a elevada qualidade de uma auditoria.

De acordo com Brender e Gauthier (2018), a Blockchain irá provocar uma mudança de paradigma em que, por um lado, a missão da auditoria irá passar de certificar as desmonstrações financeiras para testar a informação dos sistemas e, por outro, certificar a

correta implementação de blockchain. Os autores ainda mencionam uma entrevista a um Sócio da EY de Financial Services, Andreas Toggwyler, que indicou que

> [c]ertifying the blockchain would allow us to stop performing tests that seek to confirm the existence, completeness, and accuracy of the transactions. However, it is important to keep in mind that blockchain would not replace the auditor's professional judgment.

A presença da componente Blockchain nos processos, nos controlos internos, nos sistemas de informação ou como tecnologia subjacente a ativos ou passivos com impacto relevante nas demonstrações financeiras de uma entidade despoleta questões relacionadas com a obtenção de evidências de auditoria num ambiente em que a tecnologia subjacente difere da até então utilizada e sobre se os auditores estão capacitados para executar o seu trabalho e responder às exigências da tecnologia no âmbito da auditoria. Charbonneau (2020) refere que nenhum guia responde a estas questões ou ajudou os auditores a identificar e responder aos riscos, presenciando-se incerteza e dificuldade na aplicação e adequação aos normativos de auditoria.

A acompanhar o conhecimento e experiência que um auditor deverá desenvolver para efetuar uma auditoria de qualidade, o órgão de gestão e os diretores de uma entidade também terão que desenvolver controlos internos suficientes e especificamente desenhados e executados para os processos subjacentes à Blockchain.

Não obstante o conhecimento e experiência do auditor relativamente à tecnologia Blockchain, este deverá desenvolver novas metodologias de auditoria e recorrer, sempre que consider necessário, a especialistas de Blockchain. Numa auditoria de criptoativos é recorrente procurar auxílio de especialistas em Blockchain e criptografia, afirma Charbonneau (p.294). O autor ainda refere que

> the educators' ability to anticipate emerging trends and train future auditors will be important to successfully implement technology friendly audit standards.

Enquanto a forma como as auditorias atualmente são conduzidas requer a validação de saldos e transações no final do período, as blockchains conseguem produzir registos das transações quase instantaneamente. Neste sentido, a Blockchain permite efetuar auditorias contínuas ao invés de o auditor aguardar pelos registos contabilísticos efetuados pela entidade (Leoni & Schmitz, 2019 e Dai & Vasarhelyi, 2017). Isto é possível pois a Blockchain permite ao auditor obter praticamente em tempo real acesso à informação contida nos *nodes* (cópias da blockchain), num formato recorrente e consistente, evitando executar testes de amostragem,

o que aumenta o nível de garantia de fiabilidade alcançado e, por conseguinte, aprimora a qualidade da auditoria (Brender & Gauthier, 2018).

Neste sentido, é possível afirmar que a Blockchain pode ser o início do fim do uso do *random sampling* pelo auditor, permitindo a verificação de todas as transações (EY, 2016), o que antevê, mais uma vez, uma melhoria na eficiência e na eficácia da condução da auditoria. O auditor desenvolveria um software que permitisse recolher todas as informações subjacentes às transações e iria acumulando-as diariamente, eliminando muito trabalho administrativo da parte dos recursos da entidade auditada e resolveria um problema conhecido da profissão de auditoria: a recolha de evidências. Desta forma também estaria-se perante uma eliminação significativa de trabalho manual de extração de informação e de atividades de preparação da auditoria, que consomem muito esforço e tempo aos auditores (Bible, Raphael, Riviello, & Taylor, 2017).

Além dos ganhos de eficiência, a utilização da Blockchain por parte da entidade auditada pode levar a um aumento da confiança na evidência de auditoria interna e externa (Rozario & Thomas, 2019).

A inovação dos instrumentos utilizados pelo auditor na execução de uma auditoria eficiente e de qualidade, é um ponto chave quando está-se perante uma entidade auditada que utilize esta tecnologia. Um dos primeiros testemunhos desta realidade, Leopold (2020), sócio da PwC Canadá na área de National Banking and Capital Markets Assurance, afirma

> [R]ecently, I have been working with our colleagues in Switzerland to develop a software tool that assists our teams in executing crypto-related audits. Given the challenge with demonstrating completeness, existence, and ownership of cryptoassets, the tool aims to provide independent, substantive evidence of the "private key and public address pairing," which is one of the pieces needed to establish ownership of cryptocurrency. It also securely interrogates the blockchain to independently and reliably gather corroborating information about blockchain transactions and balances. Our ability to audit an entity engaged in crypto activities is still very much influenced by our ability to test our client's robust control environment and the tool is just one component of our overall approach.

Se uma classe de transações de uma indústria é registada em Blockchain, é possível que os auditores dessa indústria desenvolvam um software para auditar continuamente essas transações em Blockchain, reforçam Bible, Raphael, Riviello e Taylor (2017), permitindo

que os auditores trabalhem em conjunto na mesma blockchain reduzindo assim, por exemplo, trabalho com a validação da segurança da blockchain, sendo esse trabalho efetuado apenas por um auditor.

Segundo Simões, Cavalcanti, Melo & Reis (2021), a Blockchain tem potencial para alterar a forma como hoje em dia são efetuados os registos, incluindo como as transações são iniciadas, processadas, autorizadas, registadas e reportadas. Este facto irá gerar alterações nos modelos de negócio com vista a uma maior uniformidade e transparência na comunicação e na contabilidade.

Após análise de alguns impactos que a Blockchain poderá trazer ao auditor e à sua profissão, pode-se concluir que o papel deste profissional continuará a ser relevante. A Auditoria, na opinião de Simões *et al.* (2021):

> is a substantial activity for the functioning of the securities and securities markets, as it contributes to the significant reduction of the threat of errors, inaccuracies or bias in the financial statements, which can lead investors and creditors to rely on low quality information for your decision making (Boynton *et al.*, 2002; Perez Junior *et al.*, 2011; Attie, 2010).

Em suma, as considerações de auditoria de criptoativos e dos sistemas de informação das entidades, comparadas com as considerações tradicionais, não são fundamentalmente diferentes, mas necessitam de ser aplicadas a um ambiente diferente e de maior complexidade.

De acordo com Brender e Gauthier (2018), as características da tecnologia Blockchain irão permitir que seja possível automatizar testes de auditoria, ou, pelo menos, facilitá-los, reduzindo assim o tempo das auditorias. De momento os auditores confirmam a precisão da informação financeira das entidades auditadas através da reconciliação de diferentes fontes de informação. A implementação da Blockchain irá tornar estas reconciliações desnecessárias, porque todas as transações serão registadas nesta única base de dados distribuída e imutável. Por exemplo, não será necessário que os saldos de bancos, clientes e fornecedores voltem a ser confirmados, pois o auditor, e talvez o regulador, terão acesso à informação dos auditados e dos outros participantes na blockchain em tempo real, garantindo, assim, a monitorização contínua e a rastreabilidade. Como resultado, tem-se que tarefas atuais de auditoria que não requerem conhecimentos técnicos específicos irão desaparecer, gerando ganhos de produtividade. Neste sentido, no inquérito desenvolvido por

Brender & Gauthier (2018), 65% dos entrevistados são da opinião que irão utilizar o seu tempo em tarefas de maior valor acrescentado como análises complexas de justo-valor e de risco em que aí necessitam de usar o julgamento profissional, experiência e conhecimentos (de uma indústria, por exemplo). Assim, os auditores irão poder providenciar melhores *insights* às entidades auditadas e tornarem-se parceiros estratégicos para o negócio, concluem.

De acordo com uma publicação da KPMG (Gambhir, 2018), os auditores podem ser chamados a verificar a aplicação dos protocolos e dos mecanismos de consensos, o que corresponde à validação da "*triple-entry accounting*". Aqui, o registo efetuado na blockchain irá corresponder à terceira entrada. Esta terceira entrada corresponde a uma confirmação mútua no mesmo "livro de registos" – a blockchain. Este novo registo é exemplificado na Figura 4.1.

Entidade A	
Débito	**Crédito**
1.000 €	

Entidade B	
Débito	**Crédito**
	1.000 €

Livro de registos comum (blockchain)	
Débito	**Crédito**
1.000 €	1.000 €

Figura 4.1 Ilustração de um registo contabilístico de três entradas.

Neste cenário, em que é utilizado como base para confirmação o "terceiro registo", novas ferramentas, abordagens e critérios de auditoria serão necessários para auditar ambientes de Blockchain. Neste sentido, também os comités de auditoria terão que se adaptar e garantir que, tanto as equipas de auditoria interna como externa, estão na posse dos recursos, experiência e tecnologia adequados.

Ainda Gambhir (2018, KPMG), salienta a importância da garantia de fiabilidade dada por alguém independente que irá garantir que os protocolos da blockchain são seguros e que produzem os outputs requeridos e nos quais os participantes possam confiar. Consequentemente, esta inovação irá representar um avanço das evidências a recolher para

efeitos de auditoria e impulsionar a execução de auditorias contínuas e em tempo real, através do acesso à informação da blockchain, por expemplo, via *read-only nodes*[22].

Por outro lado, por exemplo, numa transação de troca de criptomoedas por um produto, a transferência da moeda é registada na blockchain. No entanto, esta informação é insuficiente para o auditor determinar qual, e se, o produto que foi entregue ao comprador. Segundo Bible *et al.* (2017), esta hipótese revela que a transação inscrita na blockchain pode não fornecer a evidêndia de auditoria necessária para validar a natureza da transação, pelo que a transação na blockchain ainda pode ser considerada como:

- Não autorizada, fraudulenta ou ilegal;
- Executada entre partes relacionadas;
- Relacionada com outro acordo *off-chain*;
- Incorretamente registada nas demonstrações financeiras.

Além disso, muitas transações registadas nas demonstrações financeiras refletem estimativas de valores que diferem dos valores históricos. Assim, os auditores continuam a necessitar de ponderar e executar procedimentos de auditoria às estimativas do órgão de gestão.

Uma adoção generalizada de Blockchain pode levar a que sejam criados centros globais de informação por forma a que o auditor obtenha evidências de auditoria diretamente da blockchain. No entanto, a acessibilidade à informação não impede que a mesma esteja isenta de erro ou fraude. Adicionalmente, a blockchain que origina a informação, provavelmente, não será controlada pela entidade auditada, pelo que o auditor deve avaliar se a informação é fiável, recorrendo, por exemplo, à análise de controlos gerais de tecnologias de informação (GITC). Estes podem incluir uma avaliação do mecanismo de consensos e do protocolo da blockchain (considerar se o protocolo pode ser manipulado – podendo a avaliação variar de blockchains públicas para privadas).

Com a auditoria em tempo real, nasce o potencial dos auditores serem mais eficientes, proativos, adaptados e visionários, indo ao encontro das expectativas dos utilizadores das demonstrações financeiras, que procuram, além de uma opinião sobre as demonstrações

[22] Um *read-only-node* corresponde a um hardware que detém uma cópia atualizada da informação da blockchain e que tem como única fiabilidade, como o nome indica, consultar essa mesma informação que consta na blockchain.

financeiras, recomendações mais valiosas e análises mais sofisticadas (Brender & Gauthier, 2018).

As principais consequências e impactos na auditoria de ambientes de Blockchain, apresentam-se resumidos na Quadro 4.1.

Quadro 4.1 Principais impactos da tecnologia Blockchain numa auditoria financeira

O quê?	Impacto na eficiência	Impacto no Risco de Deteção	Impacto no Risco Inerente	Impacto no Risco de Controlo
Necessidade de validação da blockchain	Diminuição	Diminuição	Aumento	Aumento
Recurso a especialistas de Blockchain	Aumento	Diminuição	Sem impacto	Sem impacto
Eliminação de confirmações externas	Aumento	Diminuição	Sem impacto	Sem impacto
Auditoria contínua e em tempo real	Aumento	Diminuição	Sem impacto	Sem impacto
Triple-entry accounting	Diminuição	Diminuição	Aumento	Aumento
Validação em conjunto de uma blockchain partilhada por uma indústria	Aumento	Sem impacto	Sem impacto	Sem impacto
Fiabilidade da informação obtida de fonte independente	Sem impacto	Diminuição	Sem impacto	Diminuição
Informação insuficiente para validação da transação	Diminuição	Aumento	Aumento	Aumento
Estimativas / mensurações que não assentam em valores históricos	Sem impacto	Aumento	Aumento	Aumento

5. Considerações numa Auditoria de Blockchain

As considerações que se seguem têm em conta a prestação de serviços de auditoria financeira a entidades que tenham incorporado esta tecnologia na sua atividade, quer através de aplicações de gestão/bases de dados suportadas em Blockchain, quer pela posse de ativos ou passivos suportados em Blockchain.

De acordo com Boulianne *et al*. (2021), as firmas de auditoria apresentam-se, nos dias de hoje, hesitantes na aceitação de mandatos de empresas que detenham montantes significativos de criptoativos devido, essencialmente, ao novo enredo tecnologicamente sofisticado que apresenta fatores de risco com os quais os auditores não estão preparados para lidar. Os autores afirmam que a recusa por parte dos auditores em aceitar este tipo de trabalhos já levou a que empresas não conseguissem financiar-se e inovarem-se devido à ausência de demonstrações financeiras auditadas em tempo útil. Aconteceu a diversas cripto empresas, cujo auditor recusou emitir uma opinião sobre as demonstrações financeiras devido à perceção não quantificável e não qualificável do risco de negócio associado a estas entidades.

A complexidade e o rápido avanço do ambiente tecnológico levam a que, em certos casos, os auditores fiquem relutantes e tenham de avaliar muito bem as operações com blockchain da entidade a auditar para que possam avançar com a execução de uma auditoria. A falta de orientação teórica e de regulação, em conjunto com diversos casos de fraude neste setor, levam a que os auditores hesitem na aceitação de trabalhos desta natureza (Abreu, Aparicio, and Costa, 2018).

Neste âmbito, deve-se ter em consideração que uma auditoria financeira pode tomar contornos diferentes do habitual. Para o efeito, é necessário ter em consideração que as entidades auditadas podem ter uma relação com a tecnologia Blockchain que assume duas naturezas diferentes (ambos os casos podem ocorrer em simultâneo):

- A entidade transaciona e/ou detém criptoativos;
- A entidade utiliza a tecnologia Blockchain como sistema de informação interno.

O presente capítulo centra-se, numa primeira instância, em aprofundar alguns dos impactos da Blockchain nas diferentes fases de execução de uma auditoria, pelo que, posteriormente, serão resumidos os principais riscos associados à auditoria de Blockchain e os respetivos

controlos e procedimentos de auditoria a desenhar e a executar para mitigar esses mesmos riscos.

5.1. Aceitação e Continuação dos Trabalhos

Um dos primeiros passos da execução de uma auditoria consiste numa avaliação da entidade a auditar, quer no ponto de vista de uma primeira auditoria à mesma ou da continuação dos trabalhos em anos posteriores à primeira auditoria. Nesta fase e considerando que a entidade a auditar tem presente a tecnologia Blockchain nas suas operações, o auditor deve ponderar determinados aspetos fundamentais por forma a tomar a decisão sobre aceitar ou dar continuidade aos trabalhos a executar.

A primeira abordagem do auditor deve passar pela ponderação dos riscos associados a estes ativos e tecnologia, pela capacidade do auditor para desenhar e executar procedimentos adicionais de auditoria que permitam mitigar, com um grau de segurança razoável, os referidos riscos, pela exposição do trabalho e eventuais impactos na reputação, entre outros.

Num cômputo geral, existem dois grandes prismas de avaliação prévia a serem ponderados pelo auditor. Por um lado, a avaliação da entidade auditada enquanto organização e a respetiva finalidade de possuir um ambiente relevante da tecnologia Blockchain nas suas operações e, por outro lado, o nível de complexidade desse mesmo ambiente de Blockchain. Relativamente à primeira perspetiva, o auditor deve ter em consideração que o branqueamento de capitais é um tema que tem surgido em torno de quem executa, por exemplo, transações com criptomoedas. O fator da descentralização dos poderes que a Blockchain proporciona é um potencial mecanismo de contorno à lei (pelo menos nos atuais moldes), pelo que o auditor deve avaliar a intenção e o propósito da utilização da tecnologia Blockchain na atividade da entidade. É de lembrar que, quando se está perante uma auditoria a um ambiente de Blockchain, é natural que o mesmo corresponda a um ambiente com impacto significativo nas operações ou com movimentos financeiros materialmente relevantes.

No caso da avaliação da complexidade do ambiente de Blockchain, o auditor deverá ter em conta, essencialmente, o seu conhecimento e experiência em trabalhar com Blockchain e a magnitude das operações efetuadas pela entidade em Blockchain.

Boulianne *et al*. (2021), num estudo sobre auditoria de Blockchain, efetuaram uma série de entrevistas a profissionais de auditoria, essencialmente, de Big4, desde seniores a sócios que não são peritos em Blockchain. Concluíram que, atualmente, estes profissionais estão a resistir a exercer neste setor devido à insuficiência de conhecimentos que mitiguem os riscos associados. Apesar de considerarem que recorrer a peritos de Blockchain possa ser uma solução, a hipótese cai por terra quando se apercebem que, mesmo assim, não têm condições suficientes para supervisionar o trabalho desenvolvido pelos peritos. Os entrevistados acrescentaram que muitas das potenciais entidades a auditar são rejeitadas devido à perceção dos auditores de que se trata de entidades que demonstram desleixo ao nível dos controlos internos necessários para assegurar ocorrência de erros ou apropriação indevida de ativos e fraude. O entrevistado #13 afirma

> [a]t some point we have to say, 'Look, you want to go public. You want to have an audit. You have to have this.' ... We're comfortable at least in saying it's not just us. None of the other Big Four are going to do this either. [The client] might be able to get like some small niche boutique accounting firm to come in and look over [their] financials but unless [they've] got proper controls and a well thought out risk matrix in place, no one will accept them.

Devido aos possíveis impactos da Blockchain numa auditoria, as firmas de auditoria necessitam adotar procedimentos de aceitação e continuação das relações com as entidades auditadas que devem ter em consideração os seguintes aspetos identificados pelo Chartered Professional Accountants (2018):

Procedimentos gerais:

a) Analisar as circunstâncias em que a entidade auditada se encontra: a entidade ter iniciado pela primeira vez operações com base em Blockchain, ou ter alterado significativamente a extensão das suas atividades com Blockchain;
b) Analisar a integridade da entidade a auditar, incluindo o propósito do negócio. Aqui, o auditor deve desenvolver inquéritos e procedimentos relacionados com o propósito do negócio. Isto acontece porque tem-se tomado conhecimento de diversos casos de atividades criminosas relacionadas com as criptomoedas (branqueamento de capitais), devido ao anonimato das transações na Blockchain;
c) Obter entendimento da entidade auditada relativamente à blockchain e a aspetos relevantes de controlo interno relacionados;

d) Obter segurança de que a gestão reconhece as responsabilidades de um potencial impacto nas demonstrações financeiras e na aplicação dos normativos de relato financeiro;
e) Obter segurança de que a gestão reconhece as responsabilidades de controlos internos que reduzam a probabilidade de distorções materiais nas demonstrações financeiras;
f) Entendimento de que a entidade auditada está consciente dos impactos ao nível do relato financeiro e de que deve ter desenhado e implementado controlos relacionados com os saldos e transações (ver Capítulo 5.3 para maior desenvolvimento sobre o controlo interno). De notar que, em casos em que a entidade a auditar ainda não tenha implementado controlos (ou estes não funcionam eficazmente) para, por exemplo, rastrear as transações, será muito difícil ou até impraticável auditar essas demonstrações financeiras;
g) Avaliar o ambiente de controlo como um todo e, mais especificamente, os controlos relacionados com a titularidade de criptoativos;
h) Avaliação das competências e capacidades da equipa a envolver na auditoria, o que inclui a inclusão na equipa de auditoria de peritos em criptografia, em TI e na valorização de criptoativos.

Procedimentos específicos para criptomoedas:

a) Ter em consideração que grande parte das corretoras (para troca de moeda fiduciária por criptomoedas) ainda não se encontra sujeita à regulação que se aplica à banca (por exemplo, *Know Your Costumer* (KYC) e *Anti Money Laundering* (AML);
b) Considerar se o volume de transações é anormal para o decurso da atividade normal da entidade, e avaliar:
    a. Se gera aumento de riscos significativos;
    b. A natureza das transações e de eventuais partes relacionadas envolvidas, inquirindo o órgão de gestão para o efeito;
    c. O racional do negócio, tendo em consideração o potencial para a ocorrência de relato financeiro fraudulento ou de apropriação indevida de ativos.

No fundo, antes de aceitar o trabalho, o auditor deve avaliar se tem os recursos e as competências adequadas e se a entidade a auditar tem um propósito de negócio apropriado, as competências necessárias e um ambiente de controlo apropriado.

5.2. Obtenção de Prova de Auditoria em Ambiente de Blockchain

A fiabilidade da informação utilizada como evidência de auditoria, ou seja, a fiabilidade da evidência em si é influenciada pela fonte da informação, pela sua natureza e pelas circunstâncias em que a evidência é obtida. Neste sentido, a fiabilidade da informação extraída da blockchain depende da:

- Fonte de informação (da blockchain em questão);
- Adequação dos recursos tecnológicos utilizados pelo auditor para obter a informação (um *block explorer*[23]).

Duas características da blockchain importantes para aferir a qualidade da prova de auditoria são: (i) o protocolo criptográfico, porque um pobre protocolo ou algoritmo pode causar fraquezas na blockchain e (ii) o mecanismo de consensos utilizado, que representa/traduz a transparência da informação proporcionada pela blockchain. No caso do POW, pode-se ter como exemplo o facto de um *hash power* de elevado poder, praticamente, anular a probabilidade de um ataque de 51%, o que se traduz em maior fiabilidade da informação registada na blockchain.

No contexto de uma auditoria em ambiente Blockchain deve ser obtido um entendimento das características relevantes da mesma, cujas informações podem ser recolhidas através de:

- Documentos e informações sobre o código publicados pelos criadores da blockchain;
- Publicações técnicas e da indústria, assim como dos membros da comunidade que suporta a blockchain;
- Experiência do próprio auditor a operar um *node* (explicado abaixo);
- Discussões com, por exemplo, peritos em criptografia e/ou ciências computacionais;
- Discussões com a gestão ou com peritos.

Torna-se, assim, crítico, no âmbito da obtenção do entendimento da entidade e da sua envolvente, uma avaliação do sistema de controlo interno da entidade e, em particular dos controlos relevantes para o funcionamento da blockchain.

O auditor pode obter informação mais direta se operar o seu próprio *node* (geralmente um *node* que apenas reflete o download de todos os blocos e transações). Desta forma o auditor

[23] Ferrameta que se conecta diretamente a uma blockchain específica e permite que o usuário visualize e consulte blocos individuais, fornecendo visibilidade a qualquer uma das transações ou outras ações registadas na blockchain.

poderá cruzar as regras do protoloco com o que efetivamente está a ser registado na blockchain e, assim, testar a fonte da informação.

Um *block explorer* é um exemplo de uma tecnologia que permite navegar na informação registada na blockchain. No entanto, para isso, deve-se ter em conta os seguintes fatores:

- Avaliar a competência e reputação de quem criou o *block explorer*;
- Avaliar a sua operacionalidade (risco de leitura de informação incorreta);
- Avaliar a atualização da ferramenta consoante o meio envolvente tecnológico.

Neste contexto, faz também sentido uma firma de auditoria avaliar uma blockchain fora do contexto de uma auditoria específica, com vista a utilizar essa informação em várias auditorias que sejam impactadas por essa mesma blockchain. De acordo com a Chartered Professional Accountants (2020, janeiro (b)), essa blockchain deve ser de uso generalizado para que esse exercício seja eficaz e eficiente. É ainda necessário ter em conta que o período coberto pela avaliação da blockchain corresponde ao período abrangido pela(s) auditoria(s) que irão beneficiar dos resultados desta avaliação.

5.3. Entendimento do Controlo Interno

Considerando que a Norma Internacional de Auditoria 315 (ISA 315) exige que o auditor obtenha um entendimento dos sistemas de informação da entidade, este trata-se, pois, de um ponto primordial para a execução de uma auditoria de demonstrações financeiras com qualidade.

A aparente segurança da blockchain, não a impede de ser suscetível a riscos tecnológicos. As eficiências a ganhar com a automatização da auditoria são acompanhadas por requisitos adicionais de procedimentos associados aos riscos de um ambiente de blockchain. Aumenta, assim, a importância dos controlos de TI na obtenção de segurança razoável de que as demonstrações financeiras não se encontram materialmente distorcidas (Psaila, 2017).

A transparência e acessibilidade da blockchain pode impactar os registos contabilísticos e as práticas de garantia de fiabilidade, dependendo da adaptação do mercado e dos novos modelos e protocolos escritos/administrados (os quais devem ser monitorizados).

Apesar da blockchain prometer altos níveis de segurança, as fraudes nas transações não conseguem ser totalmente erradicadas. Em julho de 2017 um *hacker* roubou 32 milhões de dólares de Ethereum. A causa desta fraude não estava relacionada com deficiências na

tecnologia Blockchain, mas sim relacionada com a vulnerabilidade do software usado nas Ethereum *wallets*. Ou seja, em causa está a segurança dos ambientes de controlo. Por forma a proporcionar qualidade à auditoria, os trabalhos de auditoria devem inclinar-se para a avaliação da eficácia da operacionalidade dos controlos internos de TI, mas não só. No presente subcapítulo são enunciados diferentes aspetos a ter em consideração na avaliação do controlo interno da entidade auditada.

5.3.1. Entendimento dos Sistemas de Informação

O entendimento dos sistemas de informação numa auditoria financeira passa por o auditor obter uma perceção dos procedimentos adotados pela entidade, quer ao nível de sistemas manuais, quer ao nível de sistemas de TI, nos quais as transações são iniciadas, registadas, processadas, corrigidas (se necessário) e transferidas para a contabilidade geral.

No caso das criptomoedas[24] de blockchains públicas (corresponde à maioria do mercado das criptomoedas), os registos das suas transações são efetuados permanentemente na respetiva blockchain e qualquer pessoa pode aceder e agregar essas transações (Chartered Public Accountants, 2018). As transações conseguem ser monitorizadas, por exemplo, através do número identificador da transação e/ou através da *address wallet*.

É necessário esclarecer que é improvável, mas possível, que entidades transacionem ativos digitais cujo sistema criptográfico seja outro que não Blockchain. O Ripple é um exemplo de uma criptomoeda bastante transacionada que não utiliza uma blockchain no registo das suas transações.

As características de uma blockchain, mais concretamente a imutabilidade e a descentralização, requerem cuidados redobrados inéditos aquando da sua utilização. A não gestão da segurança dos criptoativos inscritos na blockchain pode levar a uma perda total desses ativos, pelo que controlos eficazes sobre o acesso às tecnologias de informação por detrás dos criptoativos são essenciais. No caso da gestão de uma blockchain privada falhar, tal pode levar a uma perda total da informação contida nessa blockchain, podendo colocar em causa a continuidade da entidade.

[24] As criptomoedas são apresentadas como exemplo porque corresponde a um exemplo prático e a uma das aplicações mais utilizadas, até à data, da tecnologia Blockchain.

Neste sentido, tem-se que, num panorama de auditoria em ambiente de blockchain, é inevitável que os sistemas de informação sejam o objeto central do trabalho do auditor.

5.3.2. Estratégia de Confiança nos Controlos

Numa auditoria financeira em ambiente de Blockchain o auditor irá necessitar extrair informação da blockchain e também determinar a sua fiabilidade. Este processo poderá incluir uma análise dos controlos gerais de tecnologias de informação (GITC) relacionados com o ambiente de Blockchain (Chartered Professional Accountants, 2017).

De acordo com o Canadian Public Accountability Board (2019), que inspecionou a aplicação dos normativos de auditoria aplicáveis no Canadá em auditorias de criptoativos, diversos auditores não obtiveram um adequado entendimento dos riscos da auditoria aquando do desenho da abordagem a seguir. O Canadian Public Accountability Board indicou, como exemplo, no caso de entidades que detinham uma larga variedade de criptoativos, o facto de alguns auditores não terem identificado os riscos aplicáveis a cada classe material de criptoativos, incluindo se a informação obtida em cada uma das blockchains correspondia a prova de auditoria aceitável. Como principal causa destas deficiências, o Canadian Public Accountability Board indicou o não envolvimento de especialistas de Blockchain e de criptografia no levantamento dos riscos e na definição da abordagem de auditoria a seguir.

Também no seguimento destas inspeções foram identificadas falhas na avaliação da fiabilidade da blockchain. Como nem todos os protocolos de blockchain são iguais, apesar de almejarem forte resiliência à adulteração das transações, não é apropriado que os auditores considerem que todos os protocolos são efetivos e que a informação registada em todas as blockchains pode ser segura.

Neste sentido, os auditores devem identificar os riscos associados à fiabilidade da informação obtida na blockchain, incluindo transações inválidas adicionadas à blockchain e transações válidas da blockchain que são posteriormente modificadas. Os auditores devem, assim, testar os atributos do protocolo da blockchain relacionados com esses riscos. No âmbito das inspeções, foram identificadas falhas significativas ao nível da identificação dos referidos riscos, sendo que a informação obtida das blockchains corresponde à principal fonte de evidência de suporte à existência e ocorrência de saldos e transações materiais de criptoativos.

Consequentemente, é esperado que o auditor recorra a especialistas de Blockchain e de criptografia para darem apoio no desenho e execução de uma abordagem de auditoria apropriada.

Apesar da tecnologia Blockchain apresentar propriedades intrínsecas de segurança, são os humanos que vão escrever o código do software que irá integrar e interagir com a blockchain. Os humanos são falíveis e corrompíveis. De acordo com a ISA 315, é exigido aos auditores um entendimento sobre os riscos específicos de TI com impacto nas demonstrações financeiras e sobre a forma como a entidade está a dar resposta a estes riscos através da implementação de controlos de TI (Psaila, 2017). Torna-se assim fundamental, em ambientes de Blockchain, executar auditorias com base em uma estratégia focada nos controlos, por forma a mitigar os riscos tecnológicos identificados através da obtenção de segurança nos controlos. Isto porque uma estratégia baseada apenas em procedimentos substantivos não é suficiente para obter confiança sobre a prova de auditoria que é extraída de uma blockchain. Neste sentido, enuncia-se um conjunto de matérias a considerar na avaliação do ambiente tecnológico por forma a assegurar uma eventual confiança nos controlos:

- Proteção dos dados pessoais;
- Existência de plano que assegure segredos valiosos das transações;
- Como determinam quais os (se alguns) registos que devem ficar fora da blockchain;
- Como lidam com as potenciais atividades ilegais oriundas de utilização de criptomoedas (anonimato dos participantes);
- Aplicação das regulamentações elegíveis dos mercados mobiliários (se aplicável);
- Metodologia de segurança da informação contida na blockchain: definição dos "*trusted*" partners, monitorização das relações do negócio e dos protocolos de cibersegurança (controlo das transações, acesso às *keys*) por forma a prevenir repercussões financeiras e de reputação;
- Avaliação da estabilidade e escalabilidade da blockchain (por exemplo, POW, POS ou *proof of authority* (POA)) e da interoperacionalidade com as demais blockchains a que a empresa recorre;
- Modo como a empresa está a proceder na adaptabilidade aos *smart contracts* e à tokenização dos ativos (substituir dados sensíveis ou ativos físicos por um número

digital ou "token" registado na blockchain e que pode ser utilizado nos *smart contracts*), por forma a capturar todas as complexidades dos contratos existentes.

5.3.3. Serviços Prestados por uma Organização de Serviços

O Canadian Public Accountability Board (2019), no seu relatório de inspeções de auditorias de criptoativos de 2019, constatou que os auditores estavam a confiar em informações externas (de *custodians* e *crypto-exchanges*) como prova de auditoria, sem avaliar a fiabilidade dessa informação (informação sobre transações de criptoativos e de registos de custódia não sujeita a procedimentos adicionais de teste). Mais concretamente, diversos auditores não obtiveram um entendimento da natureza e da relevância dos serviços prestados pelas organizações de serviços às entidades auditadas. As organizações de serviços podem executar diversos serviços no ecossistema dos criptoativos, tais como: (a) executar transações de criptoativos (corretoras), (b) deter criptoativos (fundos de investimento) ou (c) fornecer serviços de *wallet* à entidade auditada (*wallet providers*[25]), serviços estes podem apresentar uma complexidade elevada. Adicionalmente, a organização de serviços pode não ser suficientemente sofisticada, ter ambientes de controlo pouco robustos e/ou inapropriadamente desenhados.

Quando a entidade auditada obtém de terceiros serviços que são relevantes para o seu processo de relato financeiro, o auditor deve validar as asserções afetadas. Para tal, deve começar por obter um entendimento dos controlos relevantes para a auditoria. Estes controlos podem ser os estabelecidos pela entidade auditada ou pela organização de serviços (terceiro). Neste sentido e de acordo com o Chartered Professional Accountants (2021), o auditor deve:

a) Obter um entendimento da natureza dos serviços e avaliar se efetivamente corresponde a uma organização de serviços;
b) Obter um entendimento e avaliar os controlos relevantes numa organização de serviços (se aplicável).

A abordagem ao impacto das organizações de serviços em ambiente de criptoativos encontra-se descrita nos subcapítulos seguintes. Adicionalmente, no Quadro 5.3 são

[25] Definição decorrente da "*Bulgarian Prevention of Money Laundering Act 2018 (AML Act)*": Um *wallet provider* corresponde a um terceiro que fornece serviços de proteção das *private criptographic keys* na posse, armazenamento ou transferência de criptomoedas.

enumerados alguns novos riscos e controlos relevantes a considerar aquando da presença de uma organização de serviços.

5.3.3.1. Entendimento da Natureza dos Serviços e Avaliar se Efetivamente Corresponde a uma Organização de Serviços

Perante a necessidade de recorrer a organizações de serviços, o órgão de gestão deve estabelecer processos e controlos de seleção da organização de serviços e assegurar que colaboradores com as competências adequadas revejam, por exemplo, os relatórios *System and Organization Controls* (SOC) e outros controlos não incluídos nos relatórios SOC dessas entidades.

Nos casos em que a entidade auditada considere que recorre a serviços de uma organização de serviços, o auditor deve obter um entendimento relativo a:

- Como é que a entidade auditada se relaciona com a organização de serviços:
    - Natureza e significância dos serviços prestados pelo terceiro;
    - Natureza e materialidade das classes/transações processadas ou processos de reporte financeiro impactados pelo terceiro;
    - O nível de interação (dirigir e monitorizar ou autonomia total do terceiro sem controlo por parte da entidade);
    - A natureza da relação entre as entidades, incluindo pressupostos contratuais relevantes.
- Avaliar se o terceiro corresponde de facto a uma organização de serviços.

Muitos dos controlos de uma organização de serviços são considerados como parte integrante dos sistemas de informação que alimentam as demonstrações financeiras da entidade auditada.

Há entidades terceiras que prestam serviços sem que tenham autoridade para executar movimentações, pelo que não são organizações de serviços. Trata-se de uma organização de serviços quando se verifica independência na execução de processos e/ou tarefas pelo terceiro, não estes controlados pela entidade auditada.

De acordo com o Chartered Professional Accountants (2021), num ambiente de Blockchain, são exemplos de situações onde não existe uma organização de serviços:

- A entidade auditada autoriza transações a serem executadas por uma *trading platform* ou *custodian*;
- As atividades da *trading platform* ou da *custodian* limitam-se a processar transações para a conta da entidade auditada;
- Nem a *trading platform* nem a *custodian* mantêm registos contabilísticos, gerem ativos ou iniciam, registam ou processam trasações em nome da entidade auditada.

Mesmo não sendo uma organização de serviços, o auditor deve procurar obter evidência desse entendimento e documentar apropriadamente a mesma.

Algumas *trading platforms* que detêm criptoativos da entidade auditada como meio de suporte ao *trading* podem ser consideradas como *custodians*. Por exemplo, pode-se considerar como apenas uma *trading platform* (não sendo consideradas como organização de serviços), no entanto, o auditor deve considerar se se trata de uma organização de serviços, via armazenamento de criptoativos, algo que será avaliado em função da materialidade dos ativos que detém.

De acordo com a ISA 402, perante uma organização de serviços cujos controlos sejam relevantes para o relato financeiro da entidade auditada, o auditor deve procurar obter conhecimento suficiente desses controlos, de modo a proporcionar uma base para a identificação e avaliação dos riscos de distorção material e, consecutivamente, avaliar o desenho e implementação desses controlos.

5.3.3.2. Entendimento e Avaliação dos Controlos Relevantes Numa Organização de Serviços

Na avaliação dos riscos de distorção material identificados pelo auditor inerentes aos controlos de uma organização de serviços, deve ser incluída uma expectativa de que os controlos internos de uma organização de serviços são operacionalmente eficazes a dar resposta aos riscos identificados. Nestes casos, o auditor deve testar a operacionalidade desses controlos diretamente ou confiar nos testes realizados por outros auditores.

A avaliação dos controlos relevantes da organização de serviços, conforme Norma Internacional de Trabalhos de Garantia de Fiabilidade 3402 (ISAE 3402), pode ser assegurada através de um relatório SOC, emitido por um auditor independente. Este relatório pode ser do tipo 1, o qual descreve os controlos relevantes e indica se os mesmos foram adequadamente desenhados e implementados, ou do tipo (2), o qual descreve os controlos

relevantes e indica se os mesmos foram adequadamente desenhados e implementados e se funcionaram de forma eficaz no período em questão.

Fatores a considerar na avaliação do relatório SOC:

- O âmbito do trabalho;
- O tipo de relatório e a sua adequação às necessidades da auditoria;
- O período coberto pelo relatório (com foco em evidências dos controlos perto da data de fecho).

Considerando a maturidade atual das organizações de serviços de ambientes de criptoativos, um relatório SOC pode não estar disponível, ou, estando, pode não:

- Contemplar todos os controlos relevantes para a auditoria;
- Ser suficiente para o período coberto pela auditoria;
- Ser suficiente por o auditor da entidade auditada, por exemplo, não estar satisfeito com a competência do auditor emitente do relatório.

Perante relatórios SOC que se revelam como insuficientes ou inexistentes, o auditor deve avaliar se consegue executar outros procedimentos para obter evidência de auditoria apropriada e suficiente para dar resposta aos riscos de distorção material. Se não conseguir, pode ser necessário modificar a opinião, conforme indica o Chartered Professional Accountants (2021).

No caso de a avaliação do risco incluir uma expectativa de que os controlos da organização de serviços estejam a operar eficazmente e o relatório SOC tipo 2 não estar disponível, o auditor deve obter evidência da operacionalidade dos controlos através de (1) execução de testes aos controlos e/ou (2) recurso a outro auditor independente para os executar. Caso estas possibilidades não sejam exequíveis, a opinião deve ser modificada.

Caso não seja possível obter um relatório SOC[26] ou entendimentos da entidade auditada (inquéritos combinados com inspeção ou observação), o auditor deve:

- Contactar a organização de serviços e obter informações específicas;

[26] De acordo com o focus group #2 de Boulianne *et al*. (2021): "There is a question arising about the quality of the SOC 1 and SOC 2 reports that are coming out now. If we compare them to current practices in other sectors, the reports that we see in those other areas are extremely well standardized. It's very easy to see what has been being covered and what has been tested. However, for the few [SOC 1 and SOC 2 reports] that have been released in this sector, there are things missing. (...) Just because there is a SOC 1 or SOC 2 report doesn't mean that it the report should be relied upon."

- Visitar a organização de serviços e executar procedimentos necessários à obtenção de informação sobre os seus controlos relevantes;
- Usar outro auditor para executar procedimentos necessários à obtenção de informação sobre os seus controlos relevantes.

Além do entendimento e da avaliação dos controlos da organização de serviços, também é necessário considerar (e testar se apropriado) controlos complementares executados ao nível da entidade auditada (relacionados com a organização de serviços).

Perante a confirmação de que os controlos relevantes da organização de serviços estão a operar eficazmente (para os casos em que a avaliação do risco inclua essa expectativa), podem ainda ser identificados procedimentos substantivos que requeiram a obtenção de informação diretamente na organização de serviços. Nestas situações, o auditor deve avaliar a relevância e fiabilidade dessa mesma informação via julgamento professional.

No Apêndice A, é possível visualizar, como esquema resumo da presente sub-secção do capítulo, uma possível abordagem que o auditor deve aplicar no entendimento e avaliação dos controlos relevantes numa organização de serviços, mais concretamente, linhas de orientação quanto à utilização de um relatório SOC.

5.3.3.3. Novos Riscos e Controlos Relevantes numa Organização de Serviços

Conforme afirma o Chartered Professional Accountants (2021), apesar de o ambiente dos criptoativos continuar a desenvolver-se, a interação com organizações de serviços impulsiona novos riscos relevantes para os auditores. Nomeadamente, riscos relacionados com: (i) gestão de *criptographic keys*, (ii) guarda, registo e transação de criptoativos e (iii) segurança de operações em infraestruturas de TI.

Os novos riscos supramencionados são detalhados de seguida.

Gestão de *cryptographic keys*

Uma grande responsabilidade das organizações de serviços prende-se com a gestão das cryptographic *keys*, por forma a que estas não sejam comprometidas (falhas na segurança ou destruição inadvertida) ou perdidas. Isto por porque estas empresas podem, em certos casos, ser responsáveis por todo o seu ciclo de vida, desde a sua geração à sua destruição. Neste sentido e de acordo com Chartered Professional Accountants (2021), o auditor deve

questionar o seguinte quanto à existência e à robustez dos controlos internos de gestão das *cryptographic keys*:

- Quais os objetos criptográficos [27]que estão a ser geridos?
- Estão a ser usadas *cold storage* e *hot storage* (para proteção contra perda ou roubo e para acessos frequentes, respetivamente) em função do tipo de utilização das *cryptographic keys*?
- As *cryptographic keys* mais sensíveis estão desconectadas de eventuais redes existentes (exemplo: redes de conectividade internas, internet)?
- Existem sistemas físicos de segurança que proporcionem proteção adicional?
- Que tipo de controlos existem associados à segurança e ao acesso das *cryptographic keys* desde a sua criação até à sua destruição?
- Quais os controlos implementados pela entidade auditada para aceder à plataforma do terceiro, por forma a evitar roubos, transações não autorizadas ou falsificações?
- Existem controlos de segregação de funções no manuseamento das *private keys* (separação das *private cryptographic keys* em múltiplas partes, por exemplo)?
- Foram criados backups seguros para o caso de perda da *key* original?

Guarda, registo e transação de criptoativos

Com o objetivo de uma organização de serviços proporcionar serviços que permitam guardar, registar e transacionar criptoativos, estas entidades devem estar munidas de controlos que: (a) reconciliem os movimentos ocorridos na blockchain com os registos internos; (b) garantam um registo eficaz dos movimentos; (c) certifiquem a autorização e validação do cliente na execução das transações; (d) previnam a mistura de ativos de diferentes clientes[28]; e (e) que tenham em consideração ordens de transações em aberto.

Segurança de operações em infraestruturas de TI

Relativamente à avaliação das infraestruturas de TI da organização de serviços e aos controlos relacionados com os ativos da entidades auditada, o auditor deve determinar quem

[27] São exemplos, p*rivate keys*, módulos de segurança de *hardware* (computador que guarda e gera chaves criptográficas), etc.

[28] De acordo com Boulianne *et al*. (2021), um problema relacionado com a robustez dos controlos internos diz respeito à agregação, por parte da organização de serviços, de ativos de diferentes clientes numa única conta, dificultando a distinção entre transações efetuadas com ativos da entidade auditada e outras. O relatório SOC por vezes não é explícito quanto às medidas tomadas para controlar a segregação dos ativos e das transações.

detém permissões de acesso aos ativos e quais os controlos relacionados com o manuseamento desses mesmos ativos, nomeadamente:

- Como são identificados quem gere os ativos e se têm acesso privilegiado;
- A robustez das diversas infraestruturas de segurança (rede local ou numa *cloud* partilhada);
- Robustez nos procedimentos de segurança na gestão de incidentes.

5.4. Envolvimento de Especialistas de TI

Nas entrevistas realizadas por Boulianne *et al*. (2021) é apresentado o testemunho de um indivíduo experiente em auditoria e em Blockchain que, apesar da sua experiência, evidencia com preocupações relacionadas com a reputação. Como solução para esta preocupação, indica o envolvimento de especialistas para assistir o auditor na obtenção das competências necessárias (como, por exemplo, quando o auditor recorre a atuários ou avaliadores de negócios).

Um dos entrevistados afirma ainda: "He [o perito em blockchain] doesn't know what I'm doing, and I have no idea what he's doing. Outro dos entrevistados afirma:

> One of the solutions is cross-disciplinary teams. For instance, I'm the auditor, and then I'm work with an expert in computer engineering. (...) But the thing is that with some [technologists], they don't understand audit at all. They don't get it. And we end up working as two teams. You have your audit team and your IT team, and the knowledge is separate. (Interviewee #11)

Torna-se um desafio os auditores e as equipas de TI trabalharem em conjunto de forma eficiente, beneficiando a qualidade final da auditoria (Bauer & Estep, 2019).

Outros dois dos entrevistados no referido estudo, que não se consideram especialistas em Blockchain, apresentam preocupações com a falta de capacidades para escrutinar as conclusões dos especialistas, tal como exigido pela ISA 620.

A falta de envolvimento de especialistas foi identificada pelo Canadian Public Accountability Board (2019), no seu relatório de inspeções de auditorias de criptoativos de 2019, no qual concluíram não haver a presença, em grande parte dos casos, de peritos em Blockchain aquando do entendimento dos riscos de auditoria, mais concretamente na definição dos riscos subjacentes e na abordagem a tomar.

Os protocolos e criptografia associados às blockchains estão desenhados por forma a que os registos aí inseridos não sejam corrompidos. No entanto, a eficácia desse atributo varia consoante a blockchain e seria inapropriado os auditores confiarem em blockchains cuja fiabilidade não foi verificada. Neste sentido, é esperado que os auditors financeiros recorram a especialistas de Blockchain e de criptografia para auxiliar no entendimento e avaliação das blockchains onde sejam identificados riscos de distorção material, indica o Canadian Public Accountability Board (2018).

Os auditores, em conjunto com os especialistas de TI, devem identificar os atributos relevantes da blockchain, nomeadamente a criptografia, algoritmo de validação e o mecanismo de consensos, por forma a mitigar os riscos identificados e testar se a blockchain está a operar como pretendido.

Por exemplo, a Bitcoin, que tem milhares de pessoas a trabalhar para a sua blockchain, traduz-se numa maior cadeia de blocos, tendo mais pessoas no *mining*, mais *hashpower*, criptografia mais robusta, mecanismo de consensos mais robusto e uma resolução de forks mais rápida. Já outras altcoins de comunidades mais reduzidas são provavelmente mais suscetíveis devido à reduzida robustez e a um mecanismo de consenso mais fraco. É com base nas diferenças identificadas anteriormente que as blockchains devem ser validadas, caso a caso, para efeitos de auditoria, recorrendo, para tal, à ajuda dos especialistas.

Como partilhado pelo focus group #1, uma das dificuldades está na determinação da quantidade de trabalho que será envolvida na validação da própria blockchain (revisão integral do código da blockchain ou uma investigação da criptografia subjacente à blockchain – requer análise caso a caso).

Neste sentido, e no caso da validação da blockchain da Bitcoin, ter-se-ia diversas empresas de auditoria a validar a mesma blockchain. O mesmo trabalho, de grosso modo, estaria a ser efetuado em duplicado por diversas entidades. Por forma a colmatar o trabalho adicional, apresenta-se como possíveis soluções: (i) uma firma de auditoria com múltiplas entidades auditadas e que utilizem a mesma blockchain, deve ponderar validar a blockchain à data de fecho de modo reutilizar o trabalho para as diversas entidades auditadas e/ou (ii) uma entidade reguladora (por exemplo, Ordem dos Revisores Oficiais de Contas (OROC) ou Comissão do Mercado de Valores Mobiliários (CMVM)) que efetue a validação das principais blockchains utilizadas, partilhando os respetivos resultados com as entidades de auditoria.

5.5. Impactos na Validação de Asserções

Boulianne *et al*. (2021) constatam que, no que diz respeito à auditoria de entidades com montantes materiais de criptoativos, a existência e a valorização correspondem às asserções em que os auditores identificaram maiores dificuldades. Adicionalmente, verifica-se que a validação da titularidade do criptoativo corresponde ao elemento fulcral na validação da existência das rubricas em balanço.

Os subcapítulos que se seguem procuram identificar os principais aspetos – novos riscos, controlos, procedimentos e outros aspetos – a considerar aquando da validação, essencialmente, da existência (e, consequentemente, da titularidade dos criptoativos) e da valorização, mas também de outras asserções que podem ser afetadas, nomeadamente a ocorrência e a plenitude.

5.5.1. Existência (Titularidade)

Na inspeção a auditorias de criptoativos efetuada pelo Canadian Public Accountability Board (2019), no que diz respeito a entidades auditadas que detinham criptoativos próprios, foi identificado que os auditores não obtinham evidência suficiente para suportar a titularidade desses ativos. O fator do anonimato implícito nas blockchains consiste num desafio para os auditores. Isto porque se revela difícil ligar o sujeito legal (individual ou coletivo) às identidades anónimas de uma blockchain que estão representadas por um conjunto de caracteres alfanuméricos.

Aqui apresenta-se um novo risco, que consiste na possibilidade de o proprietário partilhar a sua *private key* com terceiros e, consequentemente, ambas as partes (proprietário e terceiros) afirmarem que são proprietários (titulares). Como muitos entusiastas de criptomoedas afirmam: “not your keys, not your bitcoin”.

O Canadian Public Accountability Board (2019) identificou que os auditores validaram que as entidades auditadas detinham acesso às *private keys* que controlam os ativos. Contudo, como ter acesso a algo não significa ser proprietário, os auditores falharam na obtenção de evidências para suportar a titularidade.

São fatores a ter em consideração, segundo Canadian Public Accountability Board (2019) e Boulianne *et al*. (2021), para determinar se é necessário testar a operacionalidade dos controlos relevantes para obter evidência de auditoria sobre a titularidade dos criptoativos:

- Complexidade dos processos de negócio e do ambiente de TI;
- Disponibilidade de evidência fora da blockchain;
- Volume de transações;
- Ativos detidos pela própria entidade ou a através do recuros a organizações de serviços;
- Outros identificados pelo auditor.

De acordo com o Chartered Professional Accountants (2020, janeiro (a)) e Boulianne *et al*. (2021), listam-se exemplos de controlos que o auditor deve ter em consideração na avaliação da titularidade:

- Geração inicial de *private keys* de forma segura;
- Controlos que evitem a *private key* de ser copiada, perdida, roubada ou partilhada – se está em formato *online,* em papel, num software *offline*, hot storage, etc.;
- Sistema de autorizações apropriado para a execução de transações de criptoativos;
- Segregação de funções entre quem tem acesso à *private key* e quem é responsável pela contabilidade e/ou outras responsabilidades operacionais.

Deste modo, é necessário analisar se se está perante ativos detidos pela entidade ou se são detidos pela entidade em nome de terceiros (organização de serviços/corretora). Perante esta análise, é necessário averiguar a titularidade do ativo (tradicionalmente um documento oficial). Num ambiente de Blockchain não há documentos oficiais, sendo necessária a execução de procedimentos adicionais de auditoria. Se o ativo estiver na posse de um terceiro, as preocupações direcionam-se para a entidade terceira.

Apesar dos aparentes desafios, há abordagens viáveis para auditar criptomoedas. Uma forma recomendada por diversos autores, incluindo Boulianne *et al.* (2021), passa pelo auditor efetuar uma pequena transação com a conta da entidade auditada para uma conta criada para esse propósito. Outra forma semelhante de prova criptográfica corresponde ao envio de uma mensagem criptográfica secreta. Através destes envios é possível validar que a entidade detém, pelo menos, o acesso à respetiva conta na blockchain.

Por forma a validar que a titularidade do ativo não está a ser reclamada por duas entidades distintas (por norma, a entidade auditada e a organização de serviços, ou então, a entidade auditada e outra entidade do grupo), Dagher, Bünz, Bonneau, Clark, e Boneh (2015 citados

por Boulianne *et al*., 2021)[29] sugerem que as auditorias criptográficas das duas entidades devem ser programadas para ocorrer em simultâneo. Procura-se aproximar os auditores de ambas as partes por forma a dialogar e definir uma abordagem a seguir.

Neste sentido, o focus group #1 da investigação de Boulianne *et al*. (2021) refere ainda o seguinte

> With ownership, it's not a specific procedure but rather the body of evidence that can be performed by signing messages, by testing internal controls, by understanding how the client protects passwords. The clear expectation of ownership is changing. In a traditional audit, the client represents that they own certain things. We see an invoice and we see that they own it. But did they really pay for it? Was it paid for by another company and consigned to them? We perform several procedures to feel comfortable enough to say that they have ownership at that point in time. Our expectations of what ownership means in this area is evolving.

Outro desafio pode estar na tempestividade do teste à titularidade dos criptoativos. Isto porque, se o auditor verificar que a entidade auditada detém o criptoativo um mês após a data do balanço através de assinatura de mensagens ou de envio de pequenos montantes, isto prova que a entidade auditada controla o criptoativo nessa data, mas nada diz sobre a titularidade à data do balanço. À semelhança do inventário, os auditores devem testar a titularidade dos criptoativos à data do balanço e, em caso de perda da titularidade até à data de emissão do relatório, o mesmo deve ser divulgado nas notas do anexo.

Após a titularidade estar confirmada, o auditor pode confiar na propriedade da imutabilidade da Blockchain para verificar a existência dos criptoativos, visto a Blockchain fornecer o registo completo das transações desde a sua criação. Aqui reside a nuance de que, apesar de se referir que a Blockchain é imutável, nem todas as blockchain são iguais (ver capítulo dos especialistas de TI).

A validação do registo completo das transações e, consequentemente, do saldo dos criptoativos pode ser efetuada via *block explorer*. Nestas aplicações ou websites, caso a blockchain seja de acesso público[30], o auditor pode consultar todos os movimentos das contas da blockchain, à semelhança, por exemplo, da consulta dos extratos bancários.

[29] Dagher, G. G., Bünz, B., Bonneau, J., Clark, J., and Boneh, D. (2015). *Provisions: Privacy-Preserving Proofs of Solvency for Bitcoin Exchanges*. Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO. Disponível em: https://dl.acm.org/doi/proceedings/10.1145/2810103.
[30] São exemplos os seguintes websites: http://www.blockchain.info or http://www.blockexplorer.com.

5.5.2. Valorização

Um dos grandes desafios para entidades que detenham criptoativos passa por determinar a valorização desses mesmos criptoativos à data das demonstrações financeiras ou nas datas em que os mesmos foram transacionados.

Isto acontece, frequentemente, devido à inexistência de uma cotação dos criptoativos que seja genericamente aceite e que seja usada como referência, conforme indicado pelos focus group #1, #4 e #5 das entrevistas a auditores com experiência em criptoativos levadas a cabo por Boulianne *et al*. (2021). Como analogia tem-se o caso das taxas de câmbio utilizadas à data de fecho, as quais correspondem às estipuladas pelo banco central da região geográfica da entidade auditada. No caso de criptoativos, não existe um "banco central universal" que publique cotações.

Apesar de parecer desafiante, existem precedentes semelhantes no âmbito de uma auditoria, como, por exemplo, ações de entidades não cotadas e instrumentos financeiros derivados *over-the-counter*. Os auditores devem agir em conformidade e familiarizarem-se com as corretoras quanto às criptomoedas detidas pelas entidades auditadas e validar dessa forma a valorização desses criptoativos.

Neste sentido, a entidade auditada deve implementar políticas contabilísticas, procedimentos e controlos relacionados com a valorização de criptoativos no âmbito do relato financeiro, nomeadamente no tocante ao método de valorização e aos pressupostos usados, envolvendo sempre no processo: pessoal competente, de revisão e aprovação das valorizações, respeitando a segregação de funções. A entidade auditada ainda deve implementar políticas e procedimentos que visem a obtenção de conhecimento das partes com que transaciona.

No entanto, e dada a razoável complexidade da valorização de criptoativos, o auditor ainda deve considerar os seguintes aspetos:

- O mercado dos criptoativos funciona 24/7, pelo que é necessária uma política coerente de data de fecho (às 23:59 vs fecho do business day);
- O preço a que um criptoativo é trocado pode diferir entre diferentes corretoras;
- Insuficiência de orientações normativas para a mensuração dos criptoativos;
- Diferenças entre jurisdições relativamente à clareza como são reportados os preços de mercado.

Quanto à valorização dos criptoativos, o auditor #19 entrevistado por Boulianne *et al*. (2021) opina que

> [T]o reliably determine the fair value of a cryptocurrency is to observe actual exchange transactions in the market. There's no other way to derive a fair value, because I can't look at the intrinsic value of that cryptocurrency and come up with some sort of valuation model to derive a value.

Posto isto, o auditor e a entidade auditada deparam-se com dois potenciais problemas distintos: (i) a falta de liquidez e (ii) a falta de uma cotação universal. A falta de liquidez irá sempre depender do criptoativo em causa, pois, apesar da volatilidade dificultar a valorização dos criptoativos com baixos volumes de transação, tem-se que o preço de muitos outros produtos financeiros exóticos tem vindo a ser determinado com base em modelos financeiros complexos, como indicado Boulianne *et al*. (2021), o que faz com que a valorização de determinados ativos seja de complexidade elevada, mas exequível. Quanto à falta de uma cotação universal, a solução pode passar por recorrer às diversas corretoras de criptomoedas, as quais apresentam, na sua maioria, valores muitos semelhantes e atualizados ao minuto para os mesmos criptoativos, e testar a valorização com base na comparação dos valores médios apresentados pelas corretoras de maior liquidez.

5.5.3. Ocorrência

Uma auditoria exige que as transações registadas nas demonstrações financeiras estejam suportadas por evidências que demonstrem a sua relevância, objetivo, precisão e ocorrência. De acordo com a Chartered Professional Accountants (2017), a aceitação de uma transação numa blockchain fiável pode constituir evidência de auditoria suficiente para validar a ocorrência dessa mesma transação nas demonstrações financeiras.

A aquisição de um produto em troca de bitcoin é um exemplo. Aqui, é identificável na respetiva blockchain o envio de bitcoin para o vendedor do produto. Porém, o auditor pode conseguir, ou não, determinar que o produto (ou que produto) foi efetivamente entregue, tornando-se um ponto crítico para validar a ocorrência da transação.

Adicionalmente, existe o exemplo da validação da ocorrência de rendimentos, mais concretamente, o reconhecimento de rédito. No seguimento das inspeções realizadas pelo Canadian Public Accountability Board (2019) aos auditores de criptoativos, foi identificado que as entidades envolvidas em serviços de verificação de redes de blockchain (*mining*)

receberam criptoativos (reconhecendo-os como rédito) ao completarem a verificação e a adição de um bloco à blockchain. No teste ao reconhecimento do rédito, os auditores que limitaram o seu trabalho a validar os criptoativos recebidos pelas entidades, falharam na resposta ao risco do reconhecimento do rédito, pois este podia estar materialmente distorcido devido a fraude ou a erro. Ou seja, os procedimentos de auditoria desenhados e executados pelos auditores foram considerados, pelo Canadian Public Accountability Board, como insuficientes para dar resposta ao risco de o rédito não ter ocorrido.

Uma abordagem apropriada de auditoria inclui, como proposto pelo Canadian Public Accountability Board (2019), a obtenção do entendimento de como a entidade executa as suas atividades de *mining* e testar a capacidade de computação dos equipamentos de *mining* da entidade, os padrões de consumo de eletricidade associados, os envolvimentos em *mining pools* (quando aplicáveis) e outros fatores relevantes que suportam a opinião e conclusão do auditor de que os criptoativos recebidos são propriedade da entidade (titularidade) e que estão dentro dos níveis de capacidade de produção da entidade (ocorrência).

Neste sentido, e de acordo com o Canadian Public Accountability Board (2018), o auditor deve identificar e documentar o seu entendimento quanto aos eventuais riscos relevantes relacionados com a ocorrência de transações de criptoativos, tais como: (i) transações inválidas registadas na blockchain e (ii) transações válidas registadas e subsequentemente indevidamente modificadas.

Face aos riscos descritos, a entidade deve implementar controlos e procedimentos de documentação e de verificação da atividade operacional (no exemplo referido, a atividade de *mining*), onde registem quem e quando executou, e em que *address wallet*, por forma a reduzir e a transmitir a atividade de rédito da empresa aos diversos departamentos, onde se inclui o de contabilidade.

Ao testar a ocorrência de transações de criptoativos, o auditor deve utilizar os referidos *block explorers* para rever a informação inscrita na blockchain. Além disso, os auditores devem desenhar procedimentos que assegurem que essas ferramentas estão bem desenhadas e a operar eficazmente na disponibilização da informação requerida.

5.5.4. Plenitude

Num ambiente Blockchain, todas as transações, de todos os participantes, encontram-se inseridas nessa mesma blockchain. Se o acesso às *private keys* da entidade auditada for

facultado ao auditor, o mesmo fica na posse de uma lista de todas as transações efetuadas por essas mesmas contas nas blockchain.

No entanto existe sempre a possibilidade de a entidade auditada não reportar todas as *private keys* ou contas de uma blockchain. Consequentemente, o auditor fica limitado à informação disponibilizada pela entidade auditada. Perante estas situações, os membros do focus group #4 da investigação levada a cabo por Boulianne *et al*. (2021) afirmam que

> For completeness, this is not a blockchain problem, it's a regular audit problem. We would do the search for unrecorded liabilities but instead of finding a liability that wasn't in the books, we would find a key that we didn't know about.

Face ao problema, recomenda-se que a entidade auditada implemente políticas e procedimentos que permitam centralizar, em funções específicas, toda a atividade criptográfica da entidade, tal como processos de responsabilização pela geração e controlo de *wallets* de criptoativos. Em função das políticas implementadas pela empresa, o auditor deve avaliar e testar controlos, se aplicável, e, como procedimentos alternativos, efetuar análises, como por exemplo: à natureza dos débitos e créditos bancários, de rubricas nas demonstrações financeiras de natureza indefinida, de contratos, de atas dos órgãos sociais e de reuniões de comissões e comités, inquéritos diversos, etc.

Em suma, no contexto de Blockchain e dos criptoativos verifica-se que a validação da plenitude não acarreta novidades que mereçam particular atenção do auditor, apenas passando a incorporar no julgamento profissional o factor omissão de contas em blockchain ou das respetivas *keys* de acesso, e indagar e, se aplicável, testar controlos que a entidade possa ter implementados para controlar a sua atividade criptográfica.

5.6. Resumo dos Principais Impactos

A Blockchain apresenta-se como uma fonte de informação transparente e que vem procurar reduzir o erro humano. A qualidade dos dados corresponde a outro benefício introduzido pela Blockchain. Isto porque, por um lado, trata-se de uma base de dados segura e de disponibilidade imediata e, por outro lado, a forma como está construída proporciona elevados níveis de controlo dos dados e do seu histórico.

À semelhança de outras tecnologias e outros produtos financeiros emergentes, a validação de asserções como a existência, a ocorrência e a valorização apresenta um carácter de maior

subjetividade, cujos riscos associados podem, por vezes, ser de mitigação impossível, exigindo ao auditor a qualificação do relatório de auditoria.

Apesar das complexidades associadas, a tecnologia Blockchain oferece uma oportunidade para aperfeiçoar o processo de relato financeiro e os processos de auditoria. A adoção da tecnologia pode permitir aos auditores o desenvolvimento de procedimentos para obter evidências de auditoria diretamente de blockchains, adaptando o processo de auditoria para usufruir dos benefícios desta tecnologia. Neste contexto, o auditor deve dar resposta aos riscos adicionais que a tecnologia Blockchain introduz. Outro aspeto relevante associado à tecnologia Blockchain é o contributo que a mesma dá para que o processo de auditoria se torne mais contínuo. Por último, embora esta tecnologia possa levar a um incremento significativo da automatização do processo de auditoria, os auditores continuarão a ter de aplicar julgamento profissional, sobretudo ao nível da análise de estimativas contabilísticas e outros juízos feitos pelo órgão de gestão no âmbito da preparação das demonstrações financeiras.

5.6.1. Impactos da Tecnologia Blockchain ao Nível da Avaliação do Risco

O Quadro 5.1 resume os principais impactos da tecnologia Blockchain ao nível dos procedimentos de aceitação/continuação do serviço de avaliação de risco.

Quadro 5.1 Impactos e procedimentos que mitiguem os impactos na avaliação do risco

Fase	Impactos	Procedimentos
Entendimento da entidade e da sua envolvente	Novas variáveis a considerar no entendimento da entidade e da sua envolvente	Avaliar a importância desta tecnologia para as operações da entidade e avaliar o modo como a tecnologia se relaciona com os objetivos de negócio da entidade e com a sua estratégia.
Aceitação e continuação dos trabalhos	Novas variáveis a considerar na aceitação/continuação	Avaliar: • Se o auditor detém os recursos e as competências adequadas para obter prova de auditoria apropriada e suficiente; • Se a entidade a auditar tem um propósito de negócio apropriada para adoção desta tecnologia e de critpoativos/passivos; • Se a entidade a auditar tem as competências adequadas e sistemas de controlo interno robustos para lidar com esta tecnologia.

Fase	Impactos	Procedimentos
Obtenção de Prova de Auditoria em Ambiente de Blockchain	Novo tipo de fonte de informação como prova de auditoria	Obter um entendimento das características relevantes da blockchain, nomeadamente: do protocolo criptográfico e do mecanismo de consensos usados. Quando aplicável, fiabilidade do respetivo *block explorer* usado (operacionalidades, atualidade e competência/reputação da entidade responsável pelo desenvolvimento desta ferramenta).
Envolvimento de especialistas de TI	Maior utilização de especilistas	Assegurar que os especialistas trazem para a equipa do trabalho as competências necessárias para assegurar a obtenção de prova de auditoria apropriada e suficiente em ambiente de Blockchain. Garantir uma integração efetiva com os especialistas de TI. Procedimentos executados por estes alinhados com as necessidades de obtenção de prova de auditoria, comunicação regular e eficaz e capacidade de supervisão por parte dos auditores.
Controlo Interno		
Entendimento dos sistemas de informação	Maior ênfase aos sistemas de informação e nas TI	Entendimento dos sistemas de informação utilizados pela entidade auditada e da forma como os mesmos se interrelacionam com a tecnologia Blockchain.
Estratégia de confiança nos controlos	Maior necessidade de obtenção de confiança em controlos	Num contexto de descentralização e desmaterialização que carateriza a tecnologia Blockchain e em que não existem evidências formais tangíveis para as transações, testes substantivos apenas dificilmente permitirão a obtenção de prova de auditoria apropriada e suficiente. Na maior parte das auditorias efetuadas neste contexto, será expectável a obtenção de confiança em controlos relacionados com a segurança de criptoativos, com acessos e com a validação da legitimidade das transações. O ambiente de controlo ao nível das práticas corporativas relacionadas com a tecnologia Blockchain é igualmente relevante no contexto da auditoria.
Serviços prestados por organizações de serviços	Maior complexidade das relações, das tecnologias usadas e dos controlos executados	Avaliar se a organização de serviços tem as competências necessárias para assegurar o adequado processamento das transações. Avaliar os controlos relevantes relacionados com os serviços prestados, com especial ênfase nos controlos relacionados com a gestão de acessos.

5.6.2. Resumo dos Novos Riscos, Controlos e Procedimentos

A tecnologia Blockchain e os ativos/passivos suportados por esta deram origem a novos riscos. Os Quadros 5.2 e 5.3 listam alguns dos principais novos riscos originados, apresentando ainda alguns exemplos de controlos e de procedimentos adicionais de auditoria direcionados para esses riscos. O Quadro 5.2 lista riscos de carácter mais genérico, enquanto o Quadro 5.3 lista riscos usualmente associados a auditorias onde são identificadas organizações de serviços (OS). Nos quadros referidos anteriormente, as asserções são identificadas da seguinte forma: Plenitude (P), Existência (E), Direitos e Obrigações (DO), Valorização e Alocação (VA), Corte (C), Ocorrência (O), Valorização (V), Apresentação e Divulgação (AD).

Quadro 5.2 Novos riscos, controlos e procedimentos

Riscos	Asserção	Controlos	Procedimentos Adicionais
Entidade detém uma *wallet* de criptoativos não reconhecida nas demonstrações financeiras (as *wallets* e *addresses* são de dificil identificação se ninguém as reclamar, dado o anonimato das mesmas).	C e P	Implementação de políticas e procedimentos que permitam centralizar, em funções específicas, toda a atividade criptográfica da entidade. Criação de procedimentos e de processos de responsabilização pela geração e controlo das *wallets* de criptoativos.	Avaliação do desenho e da implementação dos controlos relevantes. Se aplicável, teste à eficácia operacional desses controlos. Execução de testes substantivos de omissão de ativos e passivos (por exemplo, análise da natureza de débitos e créditos bancários, de rubricas nas demonstrações financeiras de natureza indefinida, de contratos, de atas dos órgãos sociais e de reuniões de comissões e comités, inquéritos diversos, …) num contexto de elevado espírito crítico e ceticismo profissional.
Perda da *private key*, tornando os criptoativos inacessíveis perpetuamente (coloca em causa o direito sobre os criptoativos aí armazenados).	DO e E	Implementação de políticas e procedimentos que permitam a recuperabilidade da *private key* (incluindo a *public key*) e, em caso de perda destas, a comunicação dessa mesma perda. Controlos de segurança de geração, armazenamento, utilização e destruição das chaves criptográficas.	Avaliação do desenho e da implementação dos controlos relevantes, incluindo os seguintes: - Procedimentos e políticas de recuperabilidade - Localização física dos dados a recuperar (guardados em *hardware*, em papel, etc.) - Segregação de funções entre quem monitoriza os ativos *vs* quem executa transações com os ativos - Monitorização contínua dos ativos e cultura de controlos de *whistleblowing*, *phishing*, etc. - Confirmação da execução de revisões periódicas da existência do acesso às *wallets* Se aplicável, teste à eficácia operacional desses controlos.

Riscos	Asserção	Controlos	Procedimentos Adicionais
Acesso não autorizado às *private keys* e roubo das mesmas (coloca em causa o direito sobre os criptoativos aí armazenados).	DO e E	Implementação de políticas e procedimentos de dois ou mais fatores de autenticação para obter acesso às *private keys*. Implementação de políticas e procedimentos na utilização das *wallets - hot wallet* para aceder às transações de criptoativos e *cold wallet* para armazenar as *private keys.* Implementação uma *hot wallet* para uma pequena porção dos seus criptoativos e uma *cold wallet* para os restantes ativos.	Avaliação do desenho e da implementação dos controlos relevantes, nomeadamente verificação da robustez dos fatores de autenticação utilizados no acesso às *private keys* e da existência de diversos tipos de *wallets* para finalidades distintas. Se aplicável, teste à eficácia operacional desses controlos.
Entidade evidencia erradamente a titularidade da *private key* e, consequentemente, dos ativos associados.	DO, O e E	Implementação de políticas e procedimentos de criação de *private keys*, documentando a sua criação no espaço e no tempo e por quem e as suas motivações de utilização. Implementação de códigos de conduta e de emissões de declarações de uso e de criação de *private keys*.	Avaliação do desenho e da implementação dos controlos relevantes. Se aplicável, teste à eficácia operacional desses controlos. Execução de uma transação com uma conta específica criada para o efeito, ou envio de mensagem encriptada para a conta a validar. Execução de validações através de um software *block explorer*. Execução dos procedimentos substantivos em data coincidente com a data de relato.
Transações não válidas que foram registadas e transações válidas que foram registadas, sendo, posteriormente, indevidamente modificadas.	O	Implementação de políticas, controlos e procedimentos de documentação e de verificação da atividade operacional (por exemplo, o registo do rédito proveniente do *mining*), onde registem quem e quando executou, e em que *wallet*, por forma a registar e a transmitir a atividade de rédito da empresa ao departamento financeiro.	Avaliação do desenho e da implementação dos controlos relevantes. Se aplicável, teste à eficácia operacional desses controlos, nomeadamente, acompanhamento de um registo contabilístico de rédito, do início ao fim do processo.
Envio de criptoativos para endereços incorretos e consequente incapacidade de recuperar os ativos.	DO	Implementação de políticas e procedimentos de: cuidados com a revisão de cada endereço antes do envio; envio uma amostra antes de proceder ao envio da transação completa; utilização de QR Code ou de "copy paste"; recuperabilidade dos ativos perdidos e comunicação da eventual perda.	Avaliação do desenho e da implementação dos controlos relevantes. Se aplicável, teste à eficácia operacional desses controlos.
Falha na infraestrutura de controlos de TI resulta em perda de controlo dos criptoativos.	E e DO	Controlos gerais de TI que permitem acesso, segurança e desenvolvimento dos sistemas e alterações à gestão e às operações de TI.	Avaliação do desenho e da implementação desses controlos gerais de TI relevantes. Se aplicável, teste à eficácia operacional desses controlos.

Riscos	Asserção	Controlos	Procedimentos Adicionais
Transações com partes relacionadas não identificadas.	VA, C e AD	Implementação de políticas e procedimentos para obter conhecimento das partes com que transaciona. Atribuição de responsabilidades, dentro da entidade, pela identificação, registo, agregação e divulgação deste tipo de transações.	Avaliação do desenho e da implementação dos controlos relevantes. Se aplicável, teste à eficácia operacional desses controlos.
Atrasos significativos no processamento de transações no final do exercício (a velocidade das transações varia de blockchain para blockchain, desde segundos a vários dias, influenciando as especializações do exercício).	C	Implementação de procedimentos de monitorização de transações nos dias anteriores e posteriroes às datas de report por forma a certificar a imputação ao exercício correto.	Avaliação do desenho e da implementação dos controlos relevantes. Se aplicável, teste à eficácia operacional desses controlos. Execução de procedimentos substantivos assentes na análise de transações processadas no início do período seguinte.
Eventos ou condições que dificultam a determinação do valor a que as transações devem ser mensuradas para efeitos de relato financeiro.	V e VA	Implementação de políticas contabilísticas, de procedimentos e de controlos relacionados com a valorização de criptoativos no âmbito do relato financeiro, nomeadamente no tocante ao método de valorização e aos pressupostos usados. Envolvimento de pessoal competente no processo de valorização. Revisão e aprovação das valorizações por pessoas competentes e não envolvidas na execução das mesmas e na autorização de transações de criptoativos. Aspetos importantes a considerar: - O mercado dos criptoativos funciona 24/7, pelo que é necessária uma política coerente de data de fecho (às 23:59 vs fecho do business day). - O preço a que um criptoativo é trocado pode diferir entre diferentes corretoras. - Insuficiência de orientações normativas para a mensuração dos criptoativos. - Diferenças entre jurisdições relativamente à clareza como são reportados os preços de mercado.	Avaliação do desenho e da implementação dos controlos relevantes (incluindo, na medida do que for necessário, controlos gerais de TI). Se aplicável, teste à eficácia operacional desses controlos. Avaliação da robustez, adequação e razoabilidade das políticas contabilísticas e dos procedimentos implementados pela entidade. Execução de procedimentos substantivos de teste às valorizações (estimativas), nomeadamente: a) Quando o auditor conclui pela robustez e adequação das políticas e metodologias adotadas, confirmação da sua adequada aplicação das políticas e confirmação de que os dados usados e os cálculos estão corretos; b) Quando o auditor não consegue concluir pela robustez e adequação das políticas e metodologias adotadas, deve desenvolver uma estimativa de valor independente e comparar a mesma com a quantia escriturada.

Quadro 5.3 Novos riscos, controlos e procedimentos quando a entidade auditada recorre a uma organização de serviços

Riscos	Asserção	Controlos	Procedimentos
Seleção de uma corretora de criptoativos que não apresenta controlos eficazes.	Todas	Atribuição a pessoal competente e conhecedor dos riscos envolvidos (e de como estes devem ser mitigados) de responsabilidades pela seleção do criptoativo e da corretora. Gestor sénior deve rever e, se apropriado, aprovar as escolhas do criptoativo e da corretora. Pelo menos dois fatores de autenticação do acesso à conta da corretora.	Avaliar quem detém, opera e qual a reputação da corretora (é sabido de corretoras que influenciaram os preços de mercado via publicação de notícias artificiais). Avaliar os tipos de ativos e quais o ativos que a corretora permite comercializar, o volume de transações e de liquidez da corretora, quem selecionou o criptoativo e se a corretora apresenta um perfil adequado à tarefa. Avaliação do D&I de controlos relevantes na entidade relacionados com o relacionamento com a corretora. Se aplicável, teste à eficácia operacional desses controlos. Se necessário, análise de relatório do tipo 1 ou do tipo 2 da corretora.
Registo incorreto de criptoativos – impreciso, incompleto, não válido	Todas	A OS apresenta controlos das vendas e compras de criptoativos entre a entidade auditada e os clientes, pelos quais as transações são automaticamente registadas. A OS deve ter controlos que assegurem o rigor dos saldos e das transações dos clientes.	Análise de relatório do tipo1 ou do tipo 2 da corretora. Na ausência de relatório, o auditor deve obter entendimento destes controlos e, se aplicável testar a sua eficácia operacional.
A OS não detém criptoativos suficientes para satisfazer os depósitos da entidade auditada (risco de, na verdade, a OS não deter os criptoativos que afirma ter em sua posse).	V, E e DO	A OS executa uma reconciliação entre os criptoativos em blockchain e os seus registos internos.	Teste à reconciliação e avaliação da fiabilidade da informação proveniente da blockchain.
Falta de transparência por parte da OS relativamente às operações efetuadas com os criptoativos da entidade auditada.	E, O e V	A entidade auditada recebe uma notificação automática da OS quando uma transação é processada ou ocorrem alterações à sua conta, incluindo alterações de contactos e de suspeitas de transações não autorizadas.	Simulação de uma alteração nas contas e confirmação da receção de notificações. Simulação de uma atividade não autorizada e confirmação da adequação das notificações recebidas.
A OS não apresenta controlos efetivos associado ao processamento das transações.	V, C e E	A OS tem controlos implementados que asseguram as ordens abertas e/ou que as ordens são totalmente processadas, com precisão e atempadamente, consoante o evento que despoleta a transação.	Análise de relatório do tipo1 ou do tipo 2 da corretora. Na ausência de relatório, o auditor deve obter entendimento destes controlos e, se aplicável testar a sua eficácia operacional. Simular transações por forma a certificar a qualidade da execução de transações por parte da OS.

Riscos	Asserção	Controlos	Procedimentos
A OS não apresenta controlos apropriados que assegurem uma adequada segregação de ativos mantidos em *wallets* partilhadas ou equivalente.	V, E e DO	A OS apresenta controlos apropriados que asseguram a separação e identificação dos criptoativos que, efetivamente, são propriedade de cada um dos seus clientes. (certificação de que são os criptoativos corretos que estão a ser transacionados e armazenados).	Análise de relatório do tipo1 ou do tipo 2 da corretora. Na ausência de relatório, o auditor deve obter entendimento destes controlos e, se aplicável, testar a sua eficácia operacional.
A OS não apresenta conformidade com as políticas KYC.	E e DO	A OS apresenta controlos sobre o registo dos clientes, incluindo procedimentos de verificação de identidade aquando da abertura da conta.	Identificação da geografia da corretora e das respetivas leis e regulamentos de AML e KYC. Análise de relatório do tipo1 ou do tipo 2 da corretora, em particular no tocante aos controlos relacionados com a aceitação dos clientes por parte da OS. Na ausência de relatório, o auditor deve obter entendimento destes controlos e, se aplicável testar a sua eficácia operacional.
A OS não deteta falhas nos mecanismos de consenso.	E e DO	A OS apresenta controlos de monitorização de confirmação de que não ocorreram manipulações na blockchain.	Entendimento dos procedimentos de avaliação da blockchain e dos respetivos mecanismos de consenso e dos protocolos, por parta da OS. Análise de relatório do tipo1 ou do tipo 2 da corretora. Na ausência de relatório, o auditor deve obter entendimento destes controlos e, se aplicável testar a sua eficácia operacional.

6. Estudo Empírico – O Estado da Arte

Olhando para a as tecnologias emergentes e fazendo a ligação para a profissão da auditoria, é percetível estar-se perante o nascer de uma potencial variável que irá alterar os ambientes e/ou rubricas financeiras de algumas empresas auditadas e, por conseguinte, os processos e a metodologia utilizada na execução de uma auditoria às demonstrações financeiras.

Não se conhece a existência de estudos que conduzam a um levantamento, no panorama nacional, do grau de sensibilização dos ROC para o impacto da tecnologia Blockchain na auditoria de demonstrações financeiras. O presente estudo empírico visa, assim, suprir esta lacuna de investigação, almejando, em última instância, avaliar o estado da arte da auditoria de Blockchain e criptoativos em Portugal.

Face à crescente relevância deste fenómeno no contexto da profissão de auditoria (incluindo em Portugal), o presente estudo pretende ainda criar bases para eventuais orientações técnicas a que venham a ser emanadas pela OROC e/ou por reguladores da profissão.

O estudo empírico teve por base o envio, para todos os ROC, de um questionário com vista à recolha de informação diversa relacionada com a auditoria de Blockchain e de criptoativos. Esta informação abrangeu os seguintes tópicos relacionados com esta temática: (i) perceção da população (ROC) sobre o tema; (ii) interesse da população sobre o tema; (iii) perspetivas futuras; (iv) frequência e natureza de eventuais trabalhos, já efetuados até à data, num contexto de tecnologia de Blockchain; e (v) os principais impactos da tecnologia Blockchain nas auditorias de demonstrações financeiras (de acordo com a perceção dos ROC).

O questionário é apresentado no Apêndice B da presente dissertação.

6.1. Metodologia

O corpo do questionário foi desenvolvido em formato *online*, através da aplicação *Google Forms*. O inquérito foi alvo de um teste previamente à sua divulgação geral, tendo nessa fase sido distribuído a 5 ROC. Desta forma, foi possível recolher opiniões prévias sobre a adequação do questionário à população e proceder a correções nas perguntas e à eliminação de eventuais incongruências.

A divulgação do inquérito passou, numa primeira fase, por recolher os contactos de todos os ROC inscritos na OROC, excetuando os que se encontram suspensos, e, numa segunda e última fase, pelo envio do questionário via e-mail à população correspondente aos ROC que se encontravam em atividade. O primeiro envio do questionário ocorreu no dia 23 junho de 2022 e o segundo envio no dia 5 de julho de 2022. O período de respostas foi encerrado a 14 de julho de 2022, tendo sido obtido um total de 81 respostas elegíveis para análise, de entre os 1.370 ROC inquiridos. Por forma a mitigar o risco de respostas em duplicado, foi definido na plataforma *Google Forms* que apenas endereços de e-mail *Google* estavam elegíveis e que cada endereço apenas poderia responder uma única vez.

A aplicação específica para questionários facilitou a interação com os inquiridos, na medida em que otimizou o tempo despendido pelos mesmos. Isto porque apenas lhes foi solicitado responder a questões que verdadeiramente interessavam tendo como base as suas respostas anteriores. Mais concretamente, o questionário foi estruturado com um formato lógico que

assegurou a necessidade de resposta apenas para as questões relevantes. Por exemplo, os ROC que nunca tinham tido contacto com a tecnologia Blockchain responderam a um questionário menor do que os ROC que já haviam tido essa experiência.

Foram obtidas 81 respostas válidas, o que corresponde a uma taxa de resposta de, aproximadamente, 6%. A caraterização e a análise das respostas obtidas são apresentadas nas secções seguintes.

6.2. Estrutura do Questionário

Partindo do pressuposto que se trata de um tema emergente e cuja aplicação prática ainda se assume como escassa, a estrutura do questionário foi elaborada com vista a procurar responder a dois grandes objetivos. Por um lado, identificar o grau de sensibilização dos ROC para a tecnologia Blockchain e para os criptoativos e, por outro lado, aferir quais os principais desafios e impactos para a profissão decorrentes desta temática.

O questionário foi composto por 20 questões (ver Apêndice B). No entanto, nenhum respondente teve de responder a todas as questões. Isto porque o questionário foi estruturado com perguntas sequenciais em que, em função da resposta dada, o respondente era redirecionado para a questão seguinte mais adequada. Desta forma, foi possível separar os dois grandes grupos de respondentes: os que nunca tiveram contacto profissional com a tecnologia Blockchain e criptoativos e os que já tiveram esse contacto profissional.

Neste sentido, o inquérito foi estruturado tendo por base os seguintes três grandes grupos de respostas:

1º Grupo – Respondido por todos os inquiridos

- Se exerce a profissão de ROC;
- Dimensão da prática (volume de negócios);
- Qual o nível de conhecimento sobre a temática;
- Se procurou a aprofundar a temática;
- Se está interessado em explorar a temática;
- Se já teve oportunidades de trabalho relacionadas com entidades que detinham criptoativos ou que utilizavam a tecnologia Blockchain nos seus sistemas de informação;

2º Grupo – Respondido pelos inquiridos que tiveram oportunidades de trabalho

- Aspetos tidos em consideração no processo de aceitação e/ou rejeição de um trabalho;
- Tipo de propostas de trabalho aceites;
- Principais riscos de distorção material identificados relacionados com a tecnologia Blockchain;
- Procedimentos adicionais de auditoria desenhados e executados em resposta aos principais riscos de distorção material identificados;
- Aspetos da estratégia geral de auditoria que foram mais afetados no âmbito de trabalhos executados;
- Áreas e tópicos relacionados com a auditoria de Blockchain onde necessita de mais apoio;

3º Grupo – Respondido por todos os inquiridos

- Qualificação dos efeitos dos potenciais impactos e desafios que a tecnologia Blockchain irá colocar à profissão de auditoria;
- Qualificação dos efeitos dos potenciais impactos que a tecnologia Blockchain irá ter na forma como uma auditoria passará a ser realizada;
- Perspetiva de efetuar trabalhos num futuro próximo (até 5 anos);
- Classificação do nível atual de preparação dos auditores para executar este tipo de trabalhos;
- Classificação do nível de apoio das entidades reguladoras (CMVM, Banco do Portugal) aos auditores relativamente a estas matérias.

Face à estruturação do questionário, procurou-se desenvolver uma análise adequada a cada tipo de questões efetuadas, como explicado no subcapítulo seguinte.

6.3. Análise dos Dados

A análise dos dados foi efetuada essencialmente em Excel, tendo como pilar inicial a base de dados nesse formato extraída da aplicação *Google Forms* e que contém as respostas dos inquiridos em formato bruto.

Neste sentido, efetuou-se uma primeira análise dos dados, com carácter descritivo, onde se procurou extrair as tendências mais evidentes da população e os aspetos de maior relevo para a presente investigação. Esta análise foi efetuada transversalmente a todas as questões. Posteriormente, foi efetuada uma análise quantitativa dos dados assente em testes *t* a diferenças de médias, que permitiu aferir quanto à existência de eventuais diferenças estatisticamente significativas nas respostas obtidas junto dos vários grupos de respondentes (apurados no primeiro grupo de questões atrás descrito).

6.3.1. Caracterização dos Respondentes

É de seguida apresentada uma breve caracterização dos respondentes, tendo por base o primeiro grupo de questões incluídas no questionário atrás detalhado.

Neste sentido, verifica-se que 84% dos ROC que responderam encontram-se em atividade. Por outro lado, verifica-se que, aproximadamente, 10% dos respondentes exercem a sua atividade em empresas "Big4", conforme demonstrado no Gráfico 6.1 e, tendo em consideração que, para o ano fiscal 2021, apenas as empresas "Big4" obtiveram um volume de negócios de auditoria superior a 10 milhões de euros[31]:

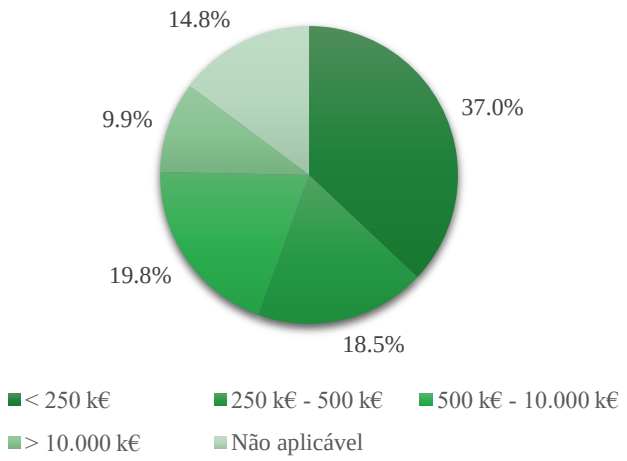


Gráfico 6.1 Distribuição dos ROC respondentes por volume de negócio da sua firma

Adicionalmente, é possível verificar que apenas 1% dos respondentes considera ter conhecimentos avançados de Blockchain e de criptoativos, face aos quase 78% que se consideram leigos ou com conhecimento básico (ver Gráfico 6.2).

[31] Conforme dados publicados nos respetivos relatórios de transparência.

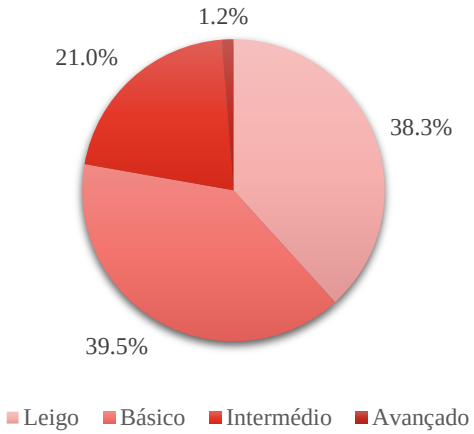


Gráfico 6.2 Nível de conhecimento sobre Blockchain e criptoativos

Por outro lado, apenas cerca de 30% dos respondentes não procuraram ainda obter conhecimentos sobre Blockchain e criptoativos e cerca de 16% não apresentam interesse em aprender mais sobre a temática (ver Apêndice C para maior detalhe).

6.3.2. Análise Quantitativa dos Dados

No que diz respeito à análise quantitativa, Sukamolson (2007) indica que esta se trata de uma representação numérica e uma manipulação de observações com o propósito de descrever e explicar o fenómeno que essas mesmas observações refletem.

A análise que se segue visa explanar a opinião dos ROC acima caracterizados, quanto ao tema em questão, procurando projetar a sensibilização dos mesmos para os principais aspetos a considerar, no presente e no futuro próximo, relacionadas, essencialmente, com trabalho de garantia de fiabilidade efetuados junto de entidades que detenham criptoativos ou que utilizem a tecnologia Blockchain.

A Tabela 6.1 explana a opinião dos 81 respondentes quanto aos potenciais impactos e desafios que a tecnologia Blockchain irá colocar à profissão de auditoria. Note-se que as opções de resposta foram graduadas de "Diminuição Significativa" (coluna 1) a "Aumento Significativo" (coluna 5) ou, "Sem bases para opinião".

De uma forma geral, os ROC que responderam reconhecem que a tecnologia Blockchain leva a um aumento (significativo) da necessidade de recurso a especialistas de TI e que leva a um aumento da eficiência do trabalho, da qualidade das auditorias, da regulação e da concentração do mercado de auditoria. Entendem ainda que as normas de auditoria vão ter de se ajustar a esta nova realidade, pelo que é expectável uma alteração nas normas. Não é

tão acentuada a tendência para o aumento dos honorários (por hora) associados nas auditorias de entidades que recorrem a tecnologia Blockchain.

A perceção de que o mercado de auditoria irá concentrar-se mais pode ter associada a ideia de que, para lidar com esta tecnologia, os auditores necessitam de desenvolver competências adicionais e que tal parece apenas estar ao alcance de poucas firmas de auditoria.

Tabela 6.1 Respostas quanto aos impactos na profissão de auditoria

	1	2	3	4	5	Sem bases para opinião
Recurso a especialistas de TI	0,0%	4,9%	4,9%	23,5%	59,3%	7,4%
Eficiência do trabalho	2,5%	6,2%	21,0%	35,8%	12,3%	22,2%
Qualidade da auditoria	1,2%	9,9%	30,9%	32,1%	9,9%	16,0%
Alterações nas normas de auditoria	0,0%	3,7%	16,0%	48,1%	18,5%	13,6%
Honorários por hora	0,0%	4,9%	30,9%	29,6%	14,8%	19,8%
Regulação	1,2%	3,7%	6,2%	40,7%	34,6%	13,6%
Concentração no mercado de auditoria	0,0%	3,7%	19,8%	44,4%	12,3%	19,8%

A Tabela 6.2 resume a opinião dos ROC inquiridos sobre os desafios e os impactos potenciais que a tecnologia Blockchain irá ter nos trabalhos de garantia de fiabilidade. Note-se que as opções de resposta foram graduadas de "Não concordo" (coluna 1) a "Concordo plenamente" (coluna 5) ou, "Sem bases para opinião".

De uma forma geral e no contexto dos trabalhos de auditoria, os ROC que responderam consideram que esta tecnologia irá levar a um maior recurso a tecnologias de informação no âmbito da execução dos procedimentos de auditoria. De igual forma, entendem que o envolvimento de especialistas (TI, avaliação, área jurídica, etc.) nos trabalhos de auditoria será cada vez maior, assim como a necessidade de obter confiança em controlos executados por organizações de serviços. Consideram ainda que o recurso a esta tecnologia irá implicar uma mais acentuada distribuição do trabalho ao longo do ano.

Adicionalmente, os ROC entendem que o surgimento desta tecnologia não terá grandes impactos ao nível da frequência da execução de procedimentos assentes em confirmações externas e ao nível do recurso a técnicas de amostragem.

Embora de forma mais ténue, os ROC que responderam entendem que os testes à eficácia operacional dos controlos serão mais relevantes no contexto de uma auditoria de Blockchain.

A menor relevância deste efeito é explicada pelo facto de uma parte significativa dos controlos relevantes para a auditoria com a tecnologia Blockchain passar a ser executada ao nível as organizações de serviços.

Tabela 6.2 Respostas quanto aos desafios e impactos nos trabalhos de garantia de fiabilidade

	1	2	3	4	5	Sem bases para opinião
Maior confiança nos controlos	6,2%	11,1%	23,5%	22,2%	19,8%	17,3%
Maior recurso a tecnologias de informação	2,5%	1,2%	6,2%	39,5%	42,0%	8,6%
Maior recurso a especialistas	2,5%	2,5%	12,3%	39,5%	33,3%	9,9%
Maior confiança em organizações de serviços	2,5%	4,9%	19,8%	45,7%	17,3%	9,9%
Menor recurso a amostragem	8,6%	21,0%	32,1%	12,3%	12,3%	13,6%
Menor recurso a confirmações externas	12,3%	21,0%	28,4%	12,3%	13,6%	12,3%
Maior distribuição de procedimentos de auditoria ao longo do ano	3,7%	8,6%	23,5%	37,0%	13,6%	13,6%

O relativamente elevado número de respostas "Sem bases de opinião" reflete, de certa forma, o número considerável de ROC com um conhecimento nulo ou baixo da tecnologia Blockchain.

O segundo grupo de questões foi apenas respondido pelos inquiridos que já se depararam com oportunidades de trabalho que envolviam a tecnologia Blockchain. Verificou-se uma dimensão muito reduzida de ROC respondentes que já tiveram esta experiência (apenas 7 respostas), o que se revela insuficiente para suportar uma análise estatística das respostas obtidas.

De acordo com os dados obtidos é ainda possível constatar que, aproximadamente, um terço (34,6%) dos inquiridos que responderam não perspetiva, num futuro próximo (até 5 anos), efetuar trabalhos em entidades com criptoativos ou que recorram à tecnologia Blockchain. Igualmente de acordo com os dados obtidos, é ainda evidente que os ROC não se sentem preparados para lidar com esta tecnologia no seu contexto profissional (77% dos ROC respondentes afirmam estar nada ou muito pouco preparados). Adicionalmente, a maior parte dos ROC que responderam ao inquérito afirma não sentirem apoio das entidades reguladoras (como a CMVM e o Banco do Portugal) relativamente a estas matérias (80% dos ROC respondentes afirmam que o referido apoio é “nenhum” ou “pouco”).

6.3.3. Validação das Hipóteses de Estudo

De uma forma geral, as respostas obtidas suportam as hipóteses objeto de estudo descritas na Capítulo 1 da presente dissertação.

Esta conclusão pode ser obtida a partir de uma observação simples dos histogramas de frequência das respostas obtidas relativamente às questões 7.1 (impacto da tecnologia Blockchain na profissão de auditoria - H1), 7.2 (impacto da tecnologia Blockchain nos trabalhos de auditoria – H2), 7.4 (preparação dos ROC para lidar com auditorias de entidades que utilizam a tecnologia Blockchain – H3) e 7.5 (apoio facultado pelos reguladores – H4). A categorização utilizada para a construção destes histogramas tem por base a escala apresentada no questionário. Mais concretamente: questões 7.1 e 7.2 (1 – impacto mínimo; 5 – impacto máximo); questão 7.4 (1 – nível mínimo de preparação; 5 – nível máximo de preparação); questão 7.5 (1 – nível mínimo de apoio; 5 – nível máximo de apoio)[32].

Os histogramas apresentam-se de seguida nas Figura 6.3, Figura 6.4, Figura 6.5 e Figura 6.6.

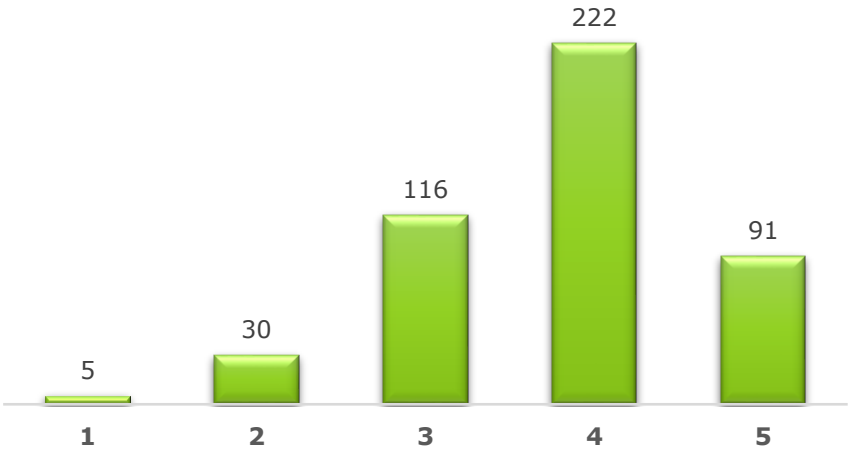


Gráfico 6.3 Impacto da tecnologia Blockchain na profissão de auditoria (questão 7.1).

[32] Para este tratamento foram omitidas as respostas "Sem bases de opinião".

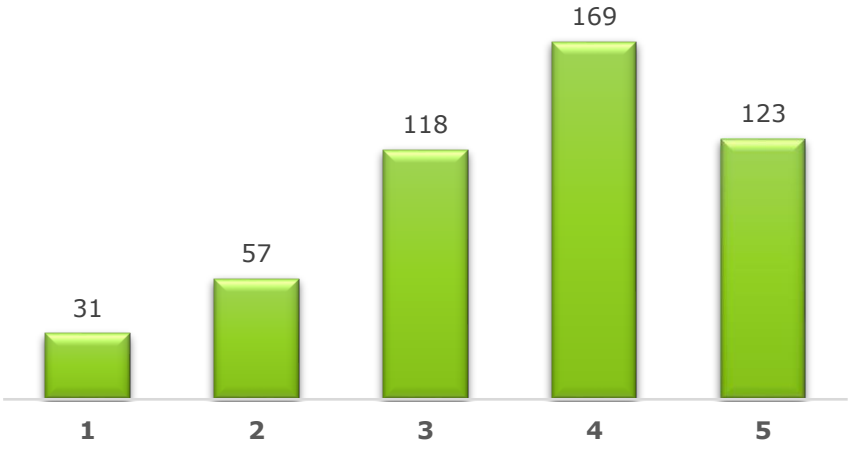


Gráfico 6.4 Impacto da tecnologia Blockchain nos trabalhos de auditoria (questão 7.2).

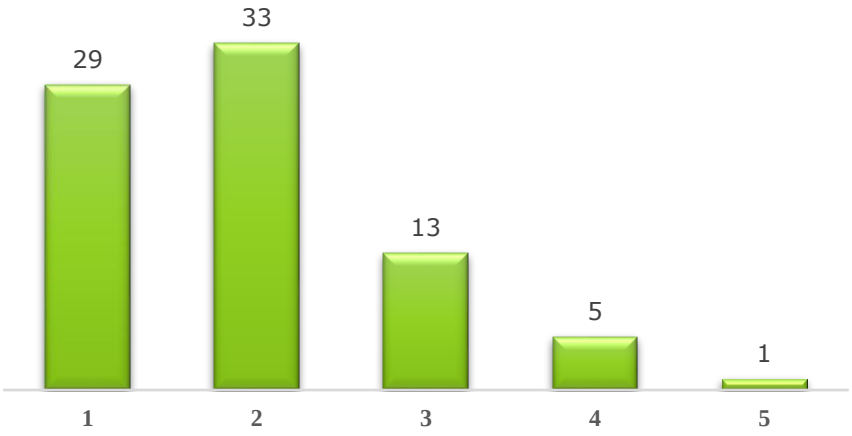


Gráfico 6.5 Preparação dos ROC para lidar com auditorias de entidades que utilizam a tecnologia Blockchain (questão 7.4).

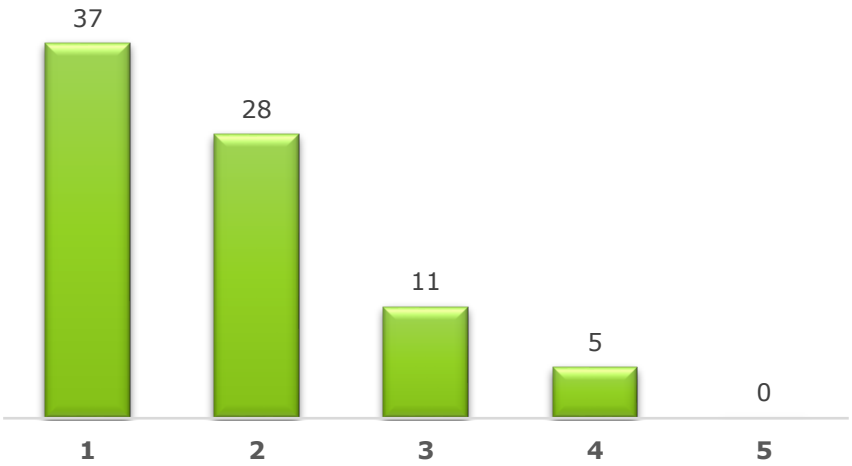


Gráfico 6.6 Apoio facultado pelos reguladores (questão 7.5).

O claro enviesamento presente nos histogramas suporta objetivamente as hipóteses em análise. Ou seja, os ROC consideram que a tecnologia Blockchain irá ter um impacto relevante na profissão e na execução das auditorias (H1 e H2), não se consideram preparados para lidar com esta temática (H3) e entendem que o apoio dado pelos reguladores e por organizações profissionais tem sido diminuto (H4).

As questões 7.1 e 7.2 foram, cada uma, subdivididas, no questionário, em oito sub-questões distintas. A análise apresentada atrás contempla as respostas agregadas obtidas para a totalidade das referidas sub-questões. Este enviesamento está igualmente presente em cada uma dessas sub-questões, conforme evidenciado no Apêndice D.

Estas conclusões foram corroboradas através de testes de hipóteses à classificação média correspondente a cada uma das questões 7.1, 7.2, 7.4 e 7.5.

Mais concretamente, para cada uma das questões em causa, foi testada a hipótese nula de que as referidas classificações médias correspondem a 2,5 (ponto médio da escala utilizada). A rejeição desta hipótese suporta as hipóteses em estudo.

Estes testes foram efetuados tendo por base a seguinte estatística-teste, para cada questão:

$$z = \frac{\overline{X} - 2{,}5}{\sqrt{\frac{S}{n}}}$$

Em que:

$z \sim N(0,1)$

$\overline{X}$ – classificação média acordo as respostas obtidas

S – desvio padrão das respostas obtidas

n – número de respostas obtidas

A Tabela 6.3 sumariza os resultados dos testes de hipótese efetuados para cada uma das questões.

Tabela 6.3 Resultados dos testes de hipótese efetuados

Questões	7.1	7.2	7.4	7.5
Média	3,78	3,59	1,96	1,80
Desvio padrão	0,87	1,16	0,94	0,90
Nº de respostas	464	498	81	81
Estatística z	31,8	28,1	-5,13	-6,97

Conforme se pode constatar, a estatística z para todas as questões encontra-se claramente na zona de rejeição (limite de rejeição de 1,64 para as questões 7.1 e 7.2 e de -1,64 para as questões 7.4 e 7.5), o que suporta as hipóteses em análise.

Ainda no âmbito do presente estudo, foi efetuada uma análise complementar no sentido de perceber se estas conclusões diferem significativamente consoante a tipologia dos respondentes. Foram efetuados testes *t* a diferenças de médias para cada caraterística relevante dos respondentes. Este tipo de teste ajusta a média das respostas tendo em consideração a dimensão das amostras e o desvio padrão, permitindo que a análise quantitativa se torne mais ilustrativa da realidade e que indique se, efetivamente, as médias observadas entre os vários grupos de características dos inquiridos evidenciam diferenças que são estatisticamente significativas, conforme Iverson, Morey, Sun, Speckman e Rouder (2009).

Os testes *t* a diferenças de médias foram efetuados tendo por base a seguinte estatística-teste para cada caraterística:

$$t = \frac{\overline{X_1} - \overline{X_2}}{\sqrt{\frac{S_1^2}{n_1} + \frac{S_2^2}{n_2}}}$$

Em que:

$t \sim t(n-2)$

$\overline{X_1}$ *e* $\overline{X_2}$ – médias das amostras 1 e 2 a comparar

S_1 *e* S_2 – desvio padrão das amostras 1 e 2

n_1 e n_2 – dimensão das amostras 1 e 2

A hipótese nula corresponde à igualdade entre médias, tendo sido considerado que as variâncias são desconhecidas e diferentes.

Cada característica do inquirido corresponde a uma questão do inquérito. Estas características, analisadas através dos testes *t*, permitem-nos verificar se, para uma dada variável, as opiniões dos inquiridos se alteram consoante as suas características. Por exemplo, face à variável "eficiência de auditoria", será que a opinião média dos ROC se altera consoante o volume de negócios da sua firma?

Seguidamente são apresentadas no Quadro 6.1 todas as características da população e todas as variáveis tidas em consideração no questionário, tal como os respetivos resultados trabalhados. Os resultados dos testes a todas as variáveis podem ser encontrados com maior detalhe nos Apêndice E e F.

Quadro 6.1 Características da população inquirida e as variáveis em análise

#	Características dos inquiridos	#	Variáveis em análise
1	Atividade vs Sem atividade	**1**	Eficiência da Auditoria
2	Big4 vs Outros	**2**	Qualidade da Auditoria
3	Conhecimento do tema vs Sem conhecimento do tema	**3**	Auditoria em tempo real
		4	Alteração nas normas de auditoria
4	Interesse pelo tema vs Sem interesse pelo tema	**5**	Honorários de Auditoria
		6	Intervenção de entidades reguladoras
5	Oportunidades de negócio vs Sem oportunidades de negócio	**7**	Concentração do mercado
		8	Maior confiança nos controlos
6	Expetativas futuras vs Sem expetativas futuras	**9**	Maior recurso a TI
		10	Maior recurso a especialistas
		11	Maior necessidade de confiar em organizações serviços
		12	Menor recurso a amostragem
		13	Menor recurso a confirmações externas
		14	Maior distribuição de procedimentos ao longo do ano
		15	Preparação dos auditores
		16	Apoio dos reguladores

Tendo por base as respostas obtidas, foram identificadas as seguintes diferenças de médias estatisticamente significativas:

Big4 vs Outros

a) Em geral, os ROC respondentes consideraram que a tecnologia Blockchain irá implicar um maior recurso a especialistas. Contudo, este efeito é mais acentuado na perspetiva dos ROC que desempenham a sua atividade no seio de uma Big4;
b) Embora com menos significância, de acordo com os ROC que desempenham a sua atividade no seio de uma Big4, a perceção de que os procedimentos de auditoria terão uma maior distribuição ao longo do ano, é mais acentuada.

Conhecimento do tema vs Sem conhecimento do tema

a) O aumento esperado na qualidade de auditoria associado à tecnologia Blockchain é maior de acordo com os inquiridos com conhecimentos intermédios/avançados;
b) O aumento esperado na eficiência dos trabalhos de auditoria associado à tecnologia Blockchain é maior de acordo com os inquiridos com conhecimentos intermédios/avançados;
c) Os inquiridos com conhecimentos intermédios/avançados, comparativamente com os inquiridos sem conhecimento do tema, consideram que os auditores estão menos mal preparados para lidar com esta temática;
d) Os inquiridos que não têm conhecimentos intermédios/avançados entendem que haverá uma maior concentração do mercado relativamente à perceção expressa pelos inquiridos com mais conhecimentos.

Interesse vs Sem Interesse

a) Os inquiridos que evidenciam mais interesse pelo tema consideram que será exigida uma maior confiança nos controlos internos da entidade auditada do que os inquiridos que não têm interesse em Blockchain e criptoativos;
b) De igual modo, os inquiridos que evidenciam mais interesse pelo tema consideram que irá haver uma maior distribuição dos procedimentos ao longo do ano e uma maior intervenção por parte dos reguladores;
c) Comparativamente com os demais inquiridos, os que demonstraram interesse pelo tema consideram que haverá um menor recurso a confirmações externas, uma maior

necessidade de confiar em organizações serviços, um maior recurso a especialistas e um maior recurso a TI. Perspetivam ainda com mais confiança a aproximação de uma abordagem de auditoria em tempo real.

Expectativas futuras

Salienta-se ainda que os ROC que têm expectativas de vir a efetuar trabalhos, num futuro próximo (5 anos), que envolvam a tecnologia Blockchain, têm uma perspetiva mais otimista quanto à preparação da profissão, quando comparada com a dos demais respondentes.

6.4. Conclusões do Inquérito

Os resultados obtidos a partir das respostas ao inquérito efetuado aos ROC confirmam as hipóteses em estudo descritas na secção 1. Mais concretamente, é entendimento dos ROC que a tecnologia Blockchain irá ter um impacto relevante na profissão em Portugal e também na forma como as auditorias são executadas (H1 e H2). É ainda entendimento dos ROC que não se encontram adequadamente preparados para lidar com esta nova realidade (H3) e que não se sentem apoiados (por reguladores e por organizações profissionais) para lidarem com auditorias de entidades que detenham criptoativos e/ou que utilizem a tecnologia Blockchain (H4).

Foram ainda identificadas algumas diferenças estatisticamente significativas nas respostas obtidas, tendo em consideração as caraterísticas dos respondentes. Estas diferenças são mais acentuadas quando se comparam os respondentes com interesse pelo tema com os que não têm interesse e quando se comparam os respondentes com conhecimento sobre o tema com os que não têm esse conhecimento.

7. Conclusão

A Blockchain apresenta-se como uma tecnologia que visa proporcionar uma fonte de informação transparente, procurando a redução do erro e interferência humana. A qualidade dos dados corresponde a outro benefício introduzido por esta tecnologia. Ou seja, trata-se de uma base de dados segura e de disponibilidade imediata, proporcionando elevados níveis de controlo dos dados e do seu histórico.

Apesar das complexidades associadas, a tecnologia Blockchain oferece uma oportunidade para aperfeiçoar o processo de relato financeiro e os processos de auditoria. A adoção desta tecnologia pode permitir aos auditores o desenvolvimento de procedimentos para obter evidências de auditoria diretamente de blockchains, adaptando o processo de auditoria para usufruir dos benefícios desta tecnologia. Neste contexto, o auditor deve dar resposta aos riscos adicionais que a tecnologia Blockchain introduz. Outro aspeto relevante associado à tecnologia Blockchain é o contributo que a mesma dá para que o processo de auditoria se torne mais contínuo. Apesar desta tecnologia permitir um incremento significativo da automatização do processo de auditoria, os auditores continuarão a ter de aplicar julgamento profissional, sobretudo ao nível da análise de estimativas contabilísticas e outros juízos feitos pelo órgão de gestão no âmbito da preparação das demonstrações financeiras.

À semelhança de outras tecnologias e outros produtos financeiros emergentes, a validação de asserções como a existência, a ocorrência e a valorização apresenta um nível de subjetividade elevado, cujos riscos associados podem, por vezes, ser de mitigação impossível, exigindo ao auditor a qualificação do relatório de auditoria (ou modificação da opinião expressa no mesmo).

Face às características da Blockchain, conclui-se, através dos inquéritos aos ROC que, no contexto português de auditoria financeira, a tecnologia Blockchain irá ter um impacto relevante na profissão e na forma como as auditorias passarão a ser executadas. Mais concretamente, os ROC perspetivam que a profissão será impactada através (i) do aumento significativo da necessidade de recurso a especialistas de TI, (ii) do maior recurso a tecnologias de informação na execução de procedimentos de auditoria, (iii) da execução da auditoria de uma forma mais distribuída ao longo do exercício económico, (iv) da adaptação dos normativos de auditoria a esta nova realidade e (v) da necessidade acrescida de obtenção de confiança em controlos executados por organizações de serviços.

A auditoria de Blockchain está numa fase emergente e cada vez mais relevante. É prova disso, o facto de cerca de dois terços dos ROC considerarem como possível efetuarem trabalhos, nos próximos 5 anos, em entidades que adotem esta tecnologia.

Outra conclusão que pode ser extraída desta investigação prende-se com a perceção evidenciada pelos ROC de que não se encontram preparados para lidar com esta nova realidade. Considerando que ainda se está numa fase embrionária desta tecnologia, e reconhecendo que se trata de questões técnicas de elevado grau de complexidade tecnológica, este resultado é perfeitamente compreensível. Uma conclusão muito relevante que se pode igualmente extrair da presente investigação prende-se com o sentido dominante (expresso por cerca de 80% dos respondentes) de que o apoio obtidos por parte de reguladores e de organizações profissionais tem sido, até à data, insuficiente.

Chama-se a atenção para o facto de este trabalho ter sido condicionado por algumas limitações relevantes, as quais devem ser tidas em consideração na análise dos resultados obtidos, nomeadamente, o facto de a taxa de respostas ao inquérito ser bastante reduzida. Esta condicionante pode prejudicar a representatividade das respostas obtidas. Por outro lado, a metodologia de análise quantitativa adotada teve por base um conjunto de julgamentos relacionados com a definição de escalas para as respostas e com pressupostos estatísticos (por exemplo, nos testes *t*), o que aumentou necessariamente a subjetividade das análises. Por último, e no que toca aos ROC que já lidaram com a tecnologia profissionalmente, não nos foi possível obter um número de respostas suficientemente robusto que viabilizasse o estudo empírico e estatístico das mesmas.

Considera-se que este trabalho constitui uma modesta, mas útil, contribuição para o debate no seio da profissão em Portugal dos impactos da tecnologia Blockchain na auditoria de demonstrações financeiras. A investigação sobre este tema não se esgota com o presente trabalho. Pelo contrário, o presente trabalho pretende dar início a um estudo mais sistemático e estruturado dos impactos da tecnologia Blockchain na auditoria, envolvendo o meio académico, a profissão, os reguladores e outros *stakeholders* relevantes. Por exemplo, seria muito interessante investigar empiricamente eventuais impactos da tecnologia Blockchain na qualidade das auditorias e na evolução do perfil dos auditores. Numa outra perspetiva, quanto à validação da asserção da existência (e titularidade do criptoativo) e, tendo em conta a complexidade, subjetividade e abrangência deste tema, seria igualmente interessante que o mesmo fosse abrangido por futuros trabalhos de investigação.

Referências Bibliográficas

Abreu, P., W., Aparicio, M. & Costa, C., J. (2018). Blockchain technology in the auditing environment. *3th Iberian Conference on Information Systems and Technologies, 1-6*. Disponível em https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8399460&isnumber=8398632.

Ahmed, Z., Cao, G., Moniz, K., Wang, C., Xue, T. & Yuan, Y. (2018). *Proof of Contribution: A Modification of Proof of Work to Increase Mining Efficiency*. IEEE International Conference on Computer Software & Applications. Key Laboratory of Trustworthy Distributed Computing and Service (BUPT): Ministry of Education Beijing, China.

Ali, A., Hassan, F., Latif, S., Kanhere, S., Qadir, J., Singh, J. *et al.* (2019). *Blockchain And The Future of the Internet: A Comprehensive Review*. Research Gate. Disponível em https://www.researchgate.net/publication/331730251_Blockchain_And_The_Future_of_the_Internet_A_Comprehensive_Review.

Andersen, N. (2016). Blockchain Technology, A game-changer in accounting? *Deloitte*. Disponível em https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/Blockchain_A%20game-changer%20in%20accounting.pdf.

Australian Accounting Standards Board (2016). *Digital Currency – A Case for Standard Setting Activity, A perspective by the AASB*. ASAF meeting, dezembro 2016.

Banco de Portugal, 12-10-2021, *O que são criptoativos?*, [Vídeo], Youtube. Disponível em https://www.youtube.com/watch?v=XMDvdgKx3EI.

Bauer, T. D., & Estep, C. (2019). One team or two? Investigating relationship quality between auditors and IT specialists: Implications for audit team identity and the audit process. *Contemporary Accounting Research, 36 (4),* 2142–2177. Disponível em https://doi.org/10.1111/19113846.12490.

Bennett, S., Charbonneau, K., Leopold, R., Mezon, L., Paradine, C., Scilipoti, A., *et al*. (2020). Blockchain and Cryptoassets: Insights from Practice. *Accounting Perspectives, 19, 4,* 283–302.

Bible, W., Raphael, J., Riviello, M. & Taylor, P. (2017). Blockchain Technology and Its Potential Impact on the Audit and Assurance Profession. Chartered Professional Accountants & American Institute of Certified Public Accountants. Disponível em https://us.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/blockchain-technology-and-its-potential-impact-on-the-audit-and-assurance-profession.pdf.

Boulianne, E., Clark, J., Eskandari, S. & Pimentel, E. (2021). Systemizing the Challenges of Auditing Blockchain-Based Assets. *Journal of Information Systems, 35, 2,* 61-75.

Brender, N. & Gauthier, M. (2018). Impacts of Blockchain on the Auditing Profession. *ISACA Journal, 5,* 27-32. Disponível em https://www.isaca.org/resources/isaca-journal/issues/2018/volume-5/impacts-of-blockchain-on-the-auditing-profession.

Broby, D. & Paul, G. (2017). Blockchain and its use in financial settlements and transactions. *The Journal of the Chartered Institute for Securities and Investment (Review of Financial Markets),* 53-55. Disponível em https://pure.strath.ac.uk/ws/portalfiles/

portal/65670933/Broby_Paul_JCISI_2017_Blockchain_and_its_use_in_financial_settlements.pdf.

Canadian Public Accountability Board (2018). *Auditing in the Crypto-Asset Sector*. Disponível em https://cpab-ccrc.ca/docs/default-source/thought-leadership-publications/2018-auditing-crypto-asset-sector-en.pdf?sfvrsn=3924e077_12.

Canadian Public Accountability Board (2019). *Auditing in the Crypto-Asset Sector Inspections Insights*. Disponível em https://www.cpab-ccrc.ca/docs/default-source/inspections-reports/2019-crypto-inspections-insights-en.pdf?sfvrsn=9aa5c0d2_20.

Catalin, C. & Gans, J. (2017, 21 de setembro). Some Simple Economics of the Blockchain. *Academia*, disponível em https://www.academia.edu/35580253/Some_Simple_Economics_of_the_Blockchain?bulkDownload=thisPaper-topRelated-sameAuthor-citingThis-citedByThis-secondOrderCitations&from=cover_page.

Charbonneau, K. (2020). How Blockchain is Disrupting the Audit: An Auditing Standard Setter's Perspective. Em The Canadian Academic Accounting Association, *Accounting Perspectives* (pp. 294-295). Disponível em https://www.researchgate.net/publication/346869951_Blockchain_and_Cryptoassets_Insights_from_Practice.

Chartered Professional Accountants (2017). Blockchain Technology and Its Potential Impact on the Audit and Assurance Profession. *CPA*. Disponível em https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/blockchain-technology-and-its-potential-impact-on-the-audit-and-assurance-profession.pdf.

Chartered Professional Accountants (2018, dezembro). Audit Considerations Related to Cryptocurrency Assets and Transactions. *CPA*. Disponível em https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/canadian-auditing-standards-cas/publications/cryptocurrency-audit-considerations.

Chartered Professional Accountants (2020, janeiro (a)). Viewpoints: Applying Canadian Auditing Standards (CASs) in the Crypto-Asset Sector, Auditing Crypto-Assets: Do You Need To Test Controls When Obtaining Audit Evidence To Support The Rights (Ownership) Assertion? *CPA*. Disponível em https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/canadian-auditing-standards-cas/publications/viewpoints-crypto-assets-ownership-assertion.

Chartered Professional Accountants (2020, janeiro (b)). Viewpoints: Applying Canadian Auditing Standards (CASs) in the Crypto-Asset Sector, Auditing Crypto-Assets: Relevance and Reliability of the Information Obtained from a Blockchain to be Used as Audit Evidence. *CPA*. Disponível em https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/canadian-auditing-standards-cas/publications/viewpoints-crypto-assets-blockchain-reliability.

Chartered Professional Accountants (2021, março). Viewpoints: Applying Canadian Auditing Standards (CASs) in the Crypto-Asset Sector, Auditing Crypto-Assets: Auditing Financial Statements of Entities That Engage With a Third-Party Service Provider In Order To Transact and/or Hold Crypto-Assets. *CPA*. Disponível em https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-

assurance/canadian-auditing-standards-cas/publications/viewpoints-crypto-assets-ownership-assertion.

Crosby, M., Kalyanaraman, V., Nachiappan, Pattanayak, P. & Verma, S. (2016). BlockChain Technology: Beyond Bitcoin. *Applied Innovation Review*, *2*. Disponível em https://j2-capital.com/wp-content/uploads/2017/11/AIR-2016-Blockchain.pdf.

Dai, J. & Vasarhelyi, M. A. (2017). Toward Blockchain-Based Accounting and Assurance. *Journal of Information Systems, 31, 3,* 5-21.

Deloitte (2018). *Deloitte's 2018 Global Blockchain Survey*. Disponível em https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/financial-services/cz-2018-deloitte-global-blockchain-survey.pdf.

Deloitte (2019). *An Internal Auditor's Guide to Blockchain: Blurring the Line Between Physical and Digital, Part I: Introduction to Blockchain*. Disponível em https://www2.deloitte.com/us/en/pages/risk/articles/internal-auditing-guide-to-blockchain.html.

Deloitte (2020). *Deloitte's 2020 Global Blockchain Survey*. Disponível em https://www2.deloitte.com/content/dam/Deloitte/mt/Documents/technology/2020-global-blockchain-survey.pdf.

Ernst & Young (2016). *Building Blocks of the Future*. Disponível em https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/digital/ey-reporting-building-blocks-of-the-future.pdf?download.

European Financial Reporting Advisory Group (2020). *Accounting for Crypto-Assets (Liabilities): Holder and Issuer Perspective.* Discussion Paper.

Forbes (2019, 18 de fevereiro). How Blockchain Can Drive Finance And Audit Performance. *Forbes*. Disponível em https://www.forbes.com/sites/insights-kpmg/2019/02/18/how-blockchain-can-drive-finance-and-audit-performance/?sh=329a43811550.

Freire, J. P. (2021). *Blockchain e Smart Contracts, Implicações Jurídicas*. Coimbra: Almedina.

Gambhir, P. (2018). The blockchain shift will be seismic. *Audit Point of View*, KPMG Canadá. Disponível em https://assets.kpmg/content/dam/kpmg/ca/pdf/2018/02/apov-blockchain-feb-2018.pdf.

Golaszewski, E., Javani, F., Sherman, A. T. & Zhang, H. (2019). On the Origins and Variations of Blockchain Technologies. *IEEE Security & Privacy*, *17*, 72-77.

Gore, I. (2020). *Valuation of Crypto-Assets*. Ramanujan College, University of Delhi, Nova Delhi, Índia. Disponível em https://www.researchgate.net/publication/341625994_valuation_of_crypto-assets.

Iverson, G., Morey, R. D., Rouder, J. N., Speckman P. L. & Sun, D. (2009). Bayesian t tests for accepting and rejecting the null hypothesis. *Psychonomic Bulletin & Review*, *16*(2), 225-237. Disponível em https://link.springer.com/content/pdf/10.3758/PBR.16.2.225.pdf.

Leoni, G. & Schmitz, J. (2019). Accounting and Auditing at the Time of Blockchain Technology: A Research Agenda. *Australian Accounting Review, 89, 29*, 331-342.

Leopold, R. (2020). The Blockchain Journey: An Auditor's Perspective. Em The Canadian Academic Accounting Association, *Accounting Perspectives* (pp. 291-294).

Disponível em https://www.researchgate.net/publication/346869951_Blockchain_and_Cryptoassets_Insights_from_Practice.

Martins, P. (2018). Introdução à Blockchain – Bitcoin, Criptomoedas, Smart Contracts, Conceitos, Tecnologia, Implicações. Lisboa: FCA.

Massachusetts Institute of Technology, MIT OpenCourseWare, 23-01-2020, *1. Introduction for 15.S12 Blockchain and Money, Fall 2018*, [Video], Youtube. Disponível em https://www.youtube.com/watch?v=EH6vE97qIP4&t=11s.

Massachusetts Institute of Technology, MIT OpenCourseWare, 12-07-2019, *8. Forks*, [Video], Youtube. Disponível em https://www.youtube.com/watch?v=U2yAcsj7P_E.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Disponível em https://bitcoin.org/bitcoin.pdf.

Nofer, M., Gomber, P., Hinz, O. & Schiereck, O. (2017). Blockchain. *Business & Information Systems Engineering*, *59*, 183–187.

Paradine, C. (2020). Auditing in a Blockchain-Enabled World: A Regulatory Perspective. Em The Canadian Academic Accounting Association, *Accounting Perspectives* (pp. 296-298). Disponível em https://www.researchgate.net/publication/346869951_Blockchain_and_Cryptoassets_Insights_from_Practice.

PricewaterhouseCoopers (2020). *6th ICO / STO Report: A Strategic Perspective, Spring 2020 Edition*. Disponível em https://www.pwc.com/ee/et/publications/pub/Strategy&_ICO_STO_Study_Version_Spring_2020.pdf.

Psaila, S. (2017). Blockchain: A game changer for audit processes? Deloitte Malta Article. Disponível em https://www2.deloitte.com/mt/en/pages/audit/articles/mt-blockchain-a-game-changer-for-audit.html.

Richins, G., Stapleton, A., Stratopoulos, T. C. & Wong, C. (2017). Big Data Analytics: Opportunity or Threat for the Accounting Profession? *Journal of Information Systems*. Disponível em https://www.researchgate.net/publication/317421884_Big_Data_Analytics_Opportunity_or_Threat_for_the_Accounting_Profession.

Rozario, A. & Thomas, C. (2019). Reengineering the Audit with Blockchain and Smart Contracts. *Journal of Emerging Technologies in Accounting, 16, 1*, 21-35.

Sayeed, S. & Marco-Gisbert, H. (2019). Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack. *Applied Sciences*, 9(9). Disponível em https://doi.org/10.3390/app9091788.

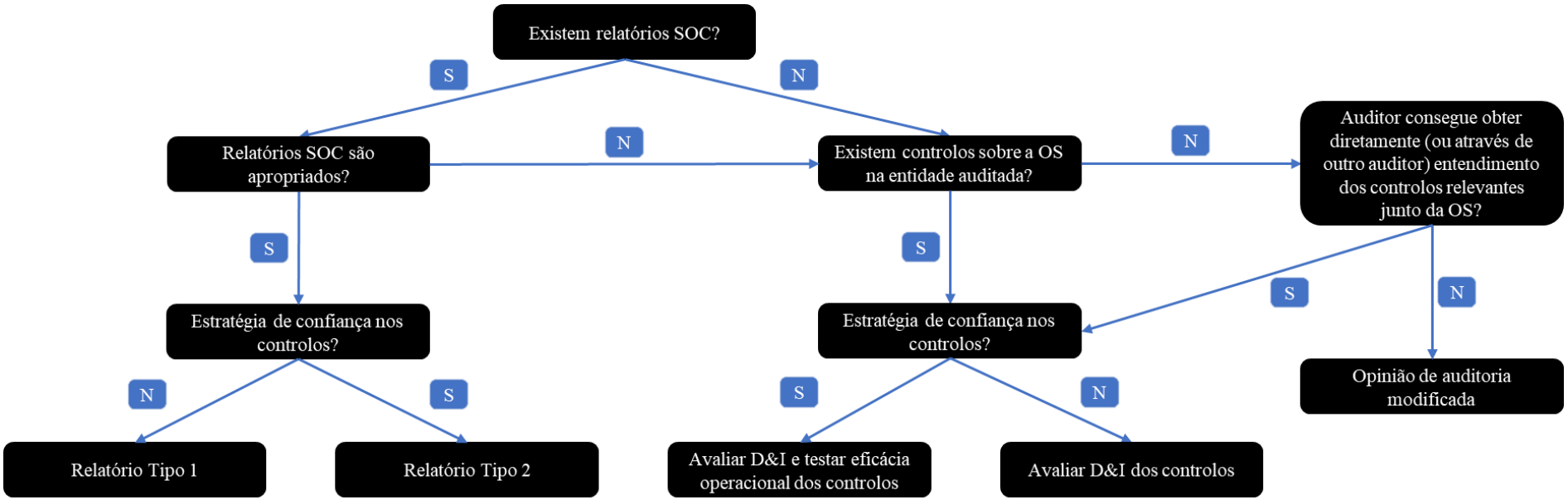
Simões, M. P., Cavalcanti, J. A., de Melo, J. F. & Reis, C. Q. (2021). Benefits of using Blockchain technology as an accounting auditing instrument. *Revista Ambiente Contábil. 13, 1,* 39-53.

Stinson, D. R. (2006). *Cryptography: Theory and Practice*. Ontario, Canada: Chapman and Hall/CRC.

Sukamolson, S. (2007). Fundamentals of quantitative research. *Language Institute, Chulalongkorn University*. Disponível em https://www.researchgate.net/profile/Vihan-Moodi/post/What_are_the_characteristics_of_quantitative_research/attachment/5f3091d0ed60840001c62a27/AS%3A922776944787456%401597018576221/download/SuphatSukamolson.pdf.

Wolfson, R. (2020, 29 de maio). The Big Four Are Gearing Up to Become Crypto and Blockchain Auditors. *Cointelegraph*, disponível em https://cointelegraph.com/news/the-big-four-are-gearing-up-to-become-crypto-and-blockchain-auditors.

Apêndice A: Utilização de Relatórios SOC



Apêndice B: Questionário

*Obrigatório

1. Encontra-se a exercer a profissão de Revisor Oficial de Contas? *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não

2. Qual o volume de negócios da prática em que exerce a profissão? *

Marcar apenas uma oval.

- ◯ < 250.000€
- ◯ 250.000€ < 500.000€
- ◯ 500.000€ < 10.000.000€
- ◯ >10.000.000€
- ◯ Não aplicável

3. Como considera o seu nível de conhecimento sobre criptoativos e/ou blockchain? *

Marcar apenas uma oval.

- ◯ Leigo
- ◯ Básico
- ◯ Intermédio
- ◯ Avançado

4. Até à data, procurou aprofundar o tema dos criptoativos e/ou blockchain? *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Residualmente

5. Está interessado em explorar o tema dos criptoativos e/ou blockchain, no contexto da auditoria? *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Talvez
- ◯ Não

6. Já teve oportunidades de trabalho (revisão legal das contas/auditoria, revisão limitada ou outros trabalhos de garantia de fiabilidade) relacionadas com entidades que detinham criptoativos ou que utilizavam a tecnologia blockchain nos seus sistemas de informação? *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não *Avançar para a pergunta 16*

6.1. Quais os aspetos que tem em consideração no processo de aceitação de um trabalho relacionado com uma entidade que adota a tecnologia Blockchain? *

Marcar tudo o que for aplicável.

- [ ] Reputação da entidade a auditar
- [ ] Honorários
- [ ] Complexidade da(s) blockchain(s) da entidade a auditar
- [ ] Os criptoativos específicos subjacentes (uma criptomoeda especifica, determinados NFT's, outros)
- [ ] Os mecanismos de consensos subjacentes
- [ ] Relevância da(s) blockchain(s) nas operações da entidade
- [ ] Competência dos recursos internos para fazer face à complexidade do ambiente tecnológico da entidade
- [ ] Ambiente regulatório a que a entidade está sujeita
- [ ] Robustez dos controlos internos tecnológicos da entidade
- [ ] Outra: _____

6.2. Já aceitou algum trabalho de uma entidade com saldos/transações de criptoativos ou com sistemas de informação baseados em blockchain? *

Marcar apenas uma oval.

- ◯ Sim *Avançar para a pergunta 11*
- ◯ Não *Avançar para a pergunta 9*

6.3. Já rejeitou algum trabalho relacionado com uma entidade que adota a tecnologia Blockchain? *

Marcar apenas uma oval.

- ◯ Sim *Avançar para a pergunta 10*
- ◯ Não *Avançar para a pergunta 15*

6.4. Quais os aspetos que teve em consideração no processo de rejeição de um trabalho relacionado com uma entidade que adota a tecnologia Blockchain? *

Marcar tudo o que for aplicável.

- [ ] Reputação da entidade a auditar/elevados níveis de exposição
- [ ] Honorários
- [ ] Complexidade da(s) blockchain(s) da entidade a auditar
- [ ] Os criptoativos específicos subjacentes (uma criptomoeda especifica, determinados NFT's, outros)
- [ ] Os mecanismos de consensos subjacentes
- [ ] Relevância da(s) blockchain(s) nas operações da entidade
- [ ] Competência dos recursos internos para fazer face à complexidade do ambiente tecnológico da entidade
- [ ] Ambiente regulatório a que a entidade está sujeita
- [ ] Robustez dos controlos internos tecnológicos da entidade
- [ ] Insuficiência de formação específica
- [ ] Outra: _____

ançar para a pergunta 16

6.3. Aceitei propostas de: *

Marcar tudo o que for aplicável.

- [ ] Revisão Legal das Contas/Auditoria
- [ ] Revisão limitada
- [ ] Trabalho de garantia de fiabilidade
- [ ] Outra: _____

6.4. Com base na sua perceção, quais os principais riscos de distorção material identificados (e respetivas asserções) relacionados com a tecnologia blockchain? *

Marcar tudo o que for aplicável.

- [ ] Recurso a uma bolsa de criptoativos que não tem controlos eficazes sobre as transações (todas as asserções)
- [ ] Wallets não registadas (plenitude)
- [ ] Incapacidade de acesso aos criptoativos em resultado da perda de private key (direitos e obrigações)
- [ ] Terceiro não autorizado obtém acesso à private key da entidade e apropria-se indevidamente dos criptoativos (existência e direitos e obrigações)
- [ ] Entidade regista criptoativos sem ter propriedade da correspondente private key (existência, ocorrência e direitos e obrigações)
- [ ] Entidade envia criptoativos para um endereço incorreto, o que inviabiliza a recuperação dos mesmos (direitos e obrigações)
- [ ] Atrasos significativos no processamento e registo de transações com criptoativos no final do período de relato (corte)
- [ ] Acontecimentos e circunstâncias que tornam difícil a mensuração dos criptoativos ou criptopassivos (rigor, valorização e imputação)
- [ ] Criptopassivos assumidos não registados (plenitude e direitos e obrigações)
- [ ] Divulgação incompleta ou incorreta (classificação e apresentação)
- [ ] Sem perceção de eventuais riscos
- [ ] Outra: _____

6.5. Quais os procedimentos adicionais de auditoria desenhados e executados em resposta aos principais riscos de distorção material identificados relacionados com a tecnologia blockchain? (selecione um máximo de 3 opções mais comuns neste contexto) *

Marcar tudo o que for aplicável.

- [ ] Obtenção de segurança relativamente a organizações de serviços
- [ ] Teste à eficácia operacional de controlos gerais informáticos
- [ ] Teste à eficácia operacional de controlos aplicacionais
- [ ] Confirmações externas
- [ ] Análise do suporte documental de transações e de criptoativos/passivos
- [ ] Reperformance de cálculos e de transações
- [ ] Teste a modelos de avaliação de criptoativos/passivos
- [ ] Simulações de acesso à blockchain e a wallets
- [ ] Análise da razoabilidade das políticas contabilísticas relacionadas
- [ ] Análise da adequação das divulgações relacionadas
- [ ] Remissão dos testes para especialistas
- [ ] Outra: _____

6.6. Quais os três aspetos da estratégia geral de auditoria que foram mais afetados no âmbito de trabalhos executados em entidades com recurso à tecnologia blockchain? *

Marcar tudo o que for aplicável.

- [ ] Maior confiança nos controlos
- [ ] Maior envolvimento de especialistas de IT
- [ ] Maior envolvimento de outros especialistas
- [ ] Maior necessidade de obtenção de segurança relativamente a organizações de serviços
- [ ] Envolvimento no trabalho de pessoas com maior senioridade
- [ ] Maior ceticismo profissional
- [ ] Outra: _____

7. Quais as áreas e tópicos relacionados com a auditoria de blockchain onde necessita de mais apoio? Escolha as 3 áreas que considera mais relevantes. *

Marcar tudo o que for aplicável.

- [ ] Relato financeiro de criptoativos/criptopassivos
- [ ] Técnicas de avaliação de criptoativos/criptopassivos
- [ ] Tecnologias de informação
- [ ] Funcionamento da tecnologia blockchain
- [ ] Natureza e funcionamento dos principais criptoativos/criptopassivos
- [ ] Controlo interno em ambiente tecnológico complexo
- [ ] Organizações de serviços no contexto de uma auditoria
- [ ] Risco de fraude no âmbito de uma auditora num ambiente com tecnologia blockchain
- [ ] Gestão de uma auditoria "em tempo real"
- [ ] Outra: _____

7.1. Com base na sua percepção, qualifique os efeitos dos potenciais impactos e desafios que a tecnologia Blockchain irá colocar à profissão de auditoria: *

Marcar apenas uma oval por linha.

	Diminuição significativa	Diminuição	Sem efeito	Aumento	Aumento significativo	Sem bases de opinião
Recurso a especialistas de IT	◯	◯	◯	◯	◯	◯
Eficiência nos trabalhos de auditoria	◯	◯	◯	◯	◯	◯
Qualidade da auditoria	◯	◯	◯	◯	◯	◯
Auditoria em tempo real	◯	◯	◯	◯	◯	◯
Alterações nos normativos de auditoria	◯	◯	◯	◯	◯	◯
Valor horário dos honorários de auditoria	◯	◯	◯	◯	◯	◯
Concentração do mercado de auditoria	◯	◯	◯	◯	◯	◯

7.2. Com base na sua perceção, qualifique os efeitos dos potenciais impactos que a tecnologia blockchain irá ter na forma como uma auditoria passará a ser realizada: (1 - não concordo; 5 - concordo plenamente) *

Marcar apenas uma oval por linha.

	1	2	3	4	5	Sem bases de opinião
Maior confiança no controlo interno	◯	◯	◯	◯	◯	◯
Maior recurso a tecnologias de informação	◯	◯	◯	◯	◯	◯
Maior recurso a especialistas	◯	◯	◯	◯	◯	◯
Maior necessidade de obter confiança em organizações de serviços	◯	◯	◯	◯	◯	◯
Menor uso de técnicas de amostragem	◯	◯	◯	◯	◯	◯
Menor recurso a confirmações externas	◯	◯	◯	◯	◯	◯
Maior distribuição dos procedimentos de auditoria ao longo do ano	◯	◯	◯	◯	◯	◯

7.3. Perspetiva num futuro próximo (até 5 anos) efetuar trabalhos (revisão legal das contas/auditoria, revisão limitada ou outros trabalhos de garantia de fiabilidade) em entidades com saldos/transações de criptoativos ou que utilizem sistemas de informação blockchain? *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Talvez
- ◯ Estou em conversações

7.4. Com base na sua perceção, classifique o nível atual de preparação dos auditores para executar trabalhos de entidades com criptoativos ou que utilizem sistemas de informação baseados em blockchain. *

Marcar apenas uma oval.

	1	2	3	4	5	
Nada preparados	◯	◯	◯	◯	◯	Muito preparados

7.5. Classifique o nível de apoio das entidades reguladoras (CMVM, Banco do Portugal) aos auditores relativamente a estas matérias. *

Marcar apenas uma oval.

	1	2	3	4	5	
Não apoiam	◯	◯	◯	◯	◯	Apoiam ao máximo

Apêndice C: Características da População Respondente

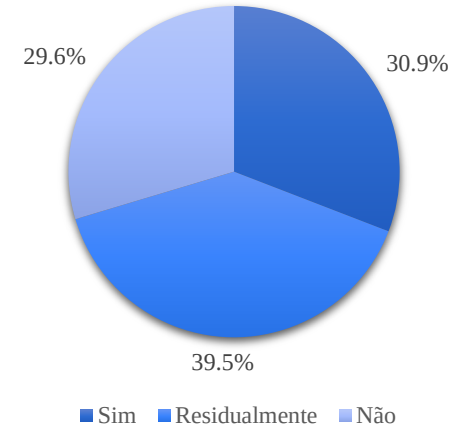


Gráfico C.1. Respondentes que procuraram obter conhecimento sobre o tema

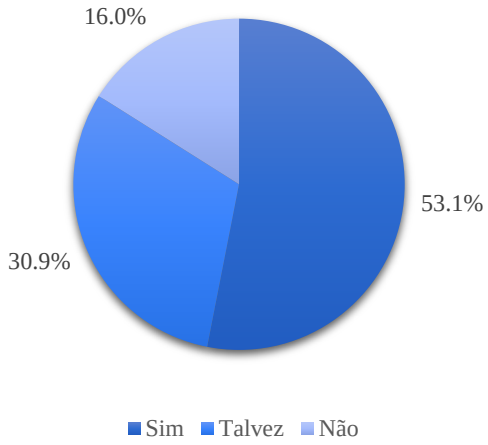


Gráfico C.2. Respondentes que apresentam interesse em explorar o tema

Apêndice D: Resultados das Subquestões

Gráfico D.1. Eficiência nos trabalhos de auditoria (questão 7.1)

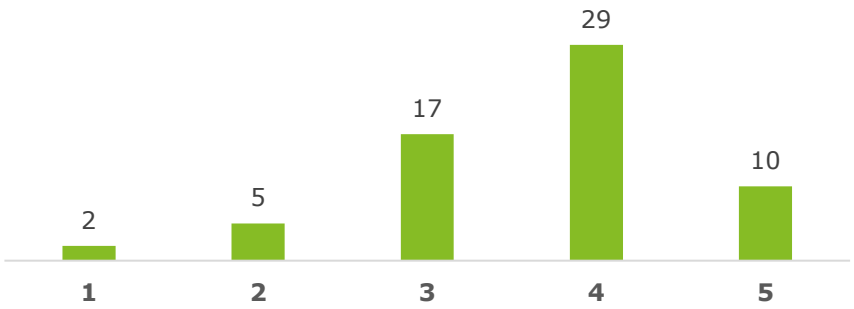


Gráfico D.2. Qualidade da auditoria (questão 7.1)

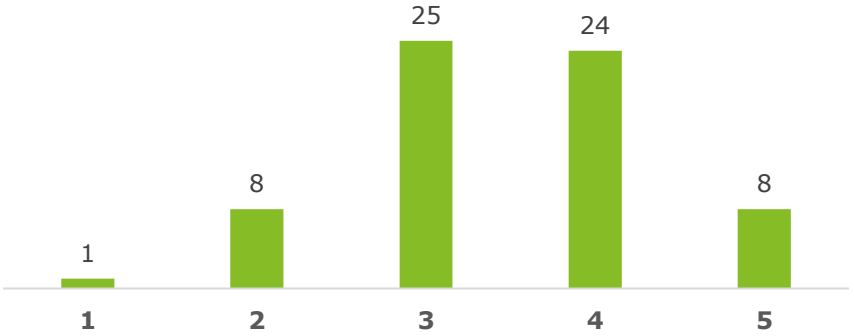


Gráfico D.3. Auditoria em tempo real (questão 7.1)

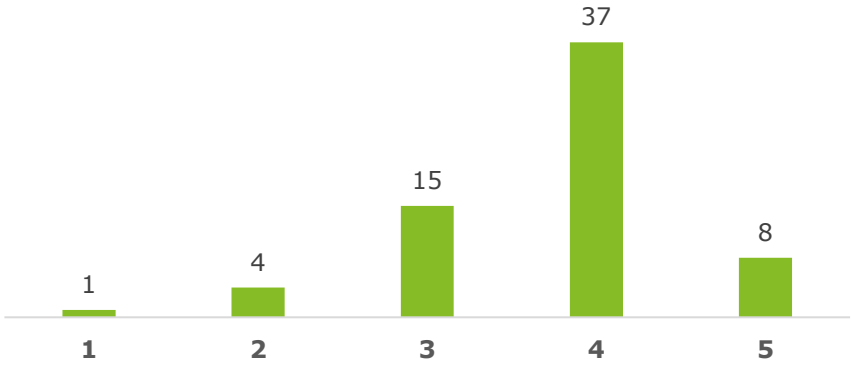


Gráfico D.4. Alterações nos normativos de auditoria (questão 7.1)

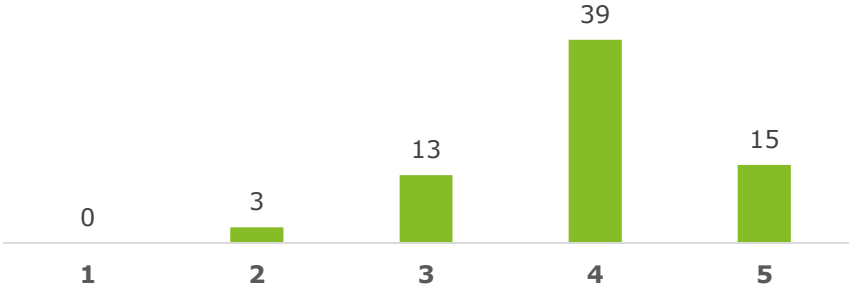


Gráfico D.5. Valor horário dos honorários de auditoria (questão 7.1)

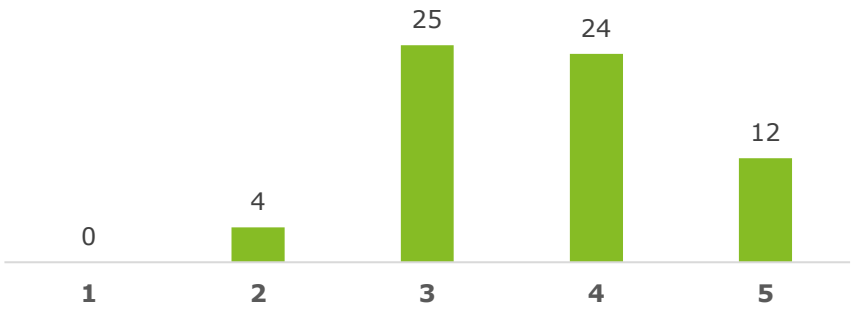


Gráfico D.6. Intervenção das entidades reguladoras (questão 7.1)

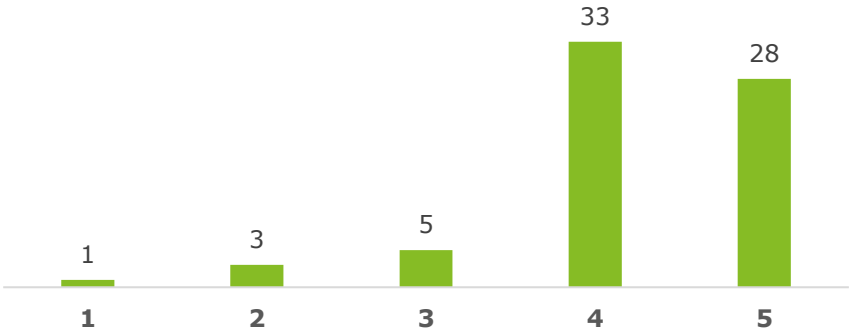


Gráfico D.7. Concentração do mercado de auditoria (questão 7.1)

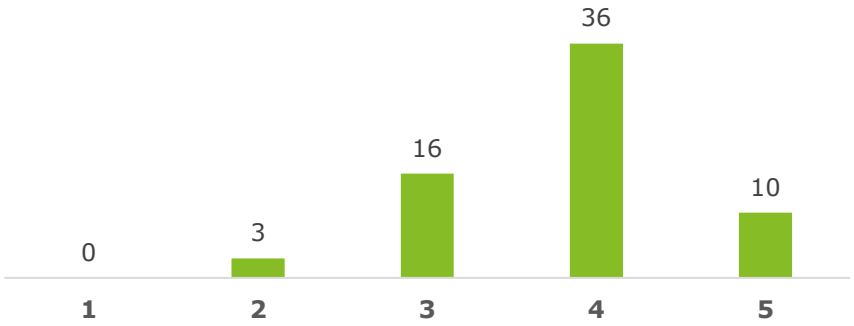


Gráfico D.8. Maior confiança no controlo interno (questão 7.2)

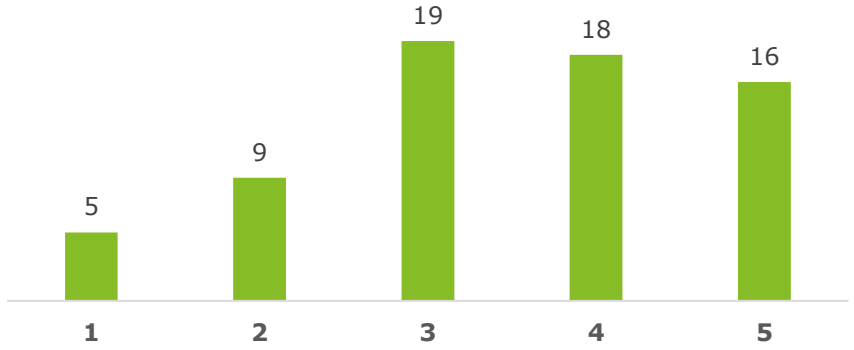


Gráfico D.9. Maior recurso a tecnologias de informação (questão 7.2)

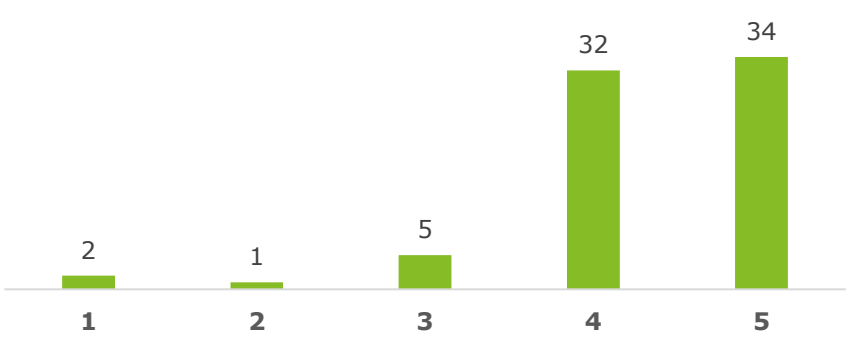


Gráfico D.10. Maior recurso a especialistas (questão 7.2)

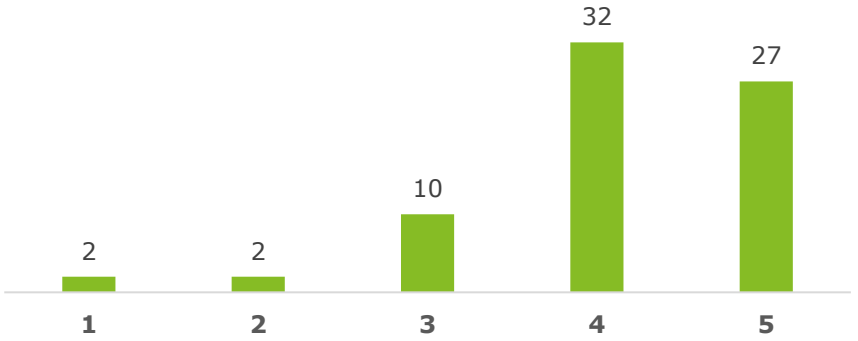


Gráfico D.11. Maior necessidade de obter confiança em organizações de serviços (questão 7.2)

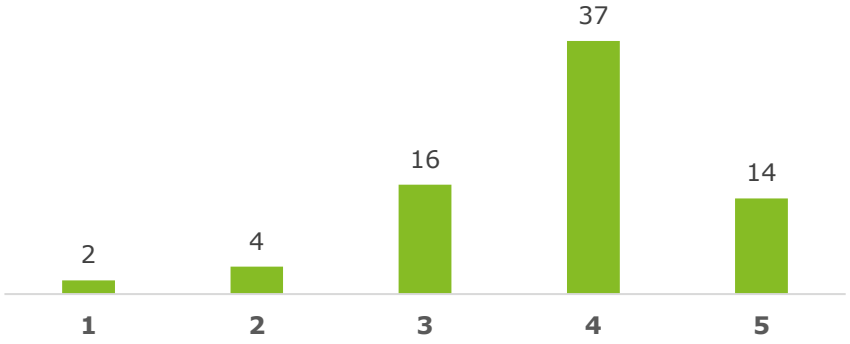


Gráfico D.12. Menor uso de técnicas de amostragem (questão 7.2)

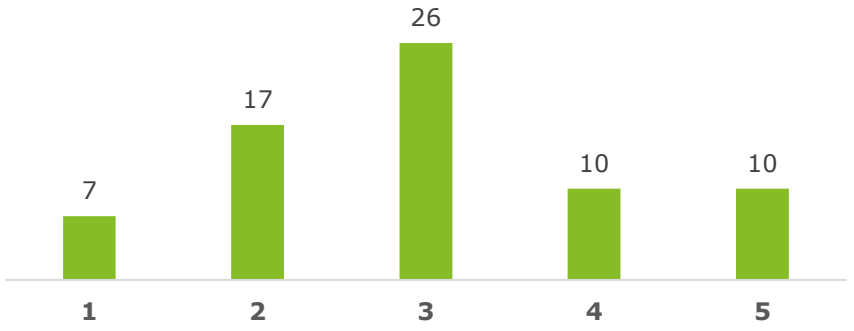


Gráfico D.13. Menor recurso a confirmações externas (questão 7.2)

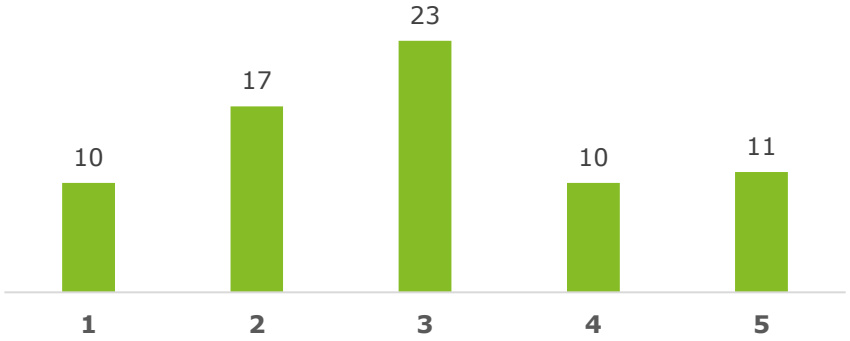
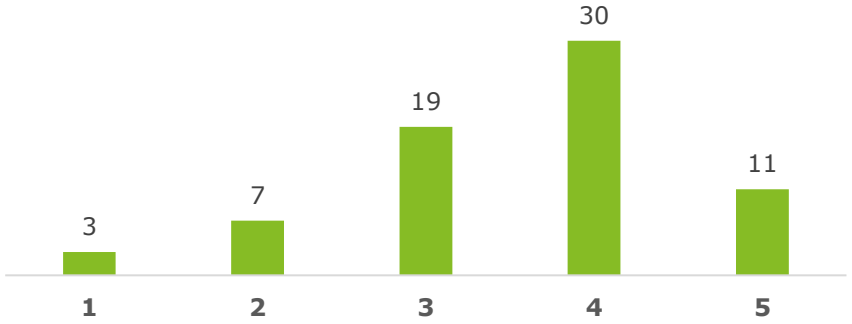


Gráfico D.14. Maior distribuição dos procedimentos de auditoria ao longo do ano (questão 7.2)



Apêndice E: Resultados dos Testes *t*

	Atividade vs Sem Atividade			Big 4 vs Non Big 4		
Questão	**P Value**	**Relação**	**Conclusão**	**P Value**	**Relação**	**Conclusão**
1	0,1444	> 0	Rejeitar	0,1781	> 0	Rejeitar
2	0,2393	> 0	Rejeitar	0,3802	> 0	Rejeitar
3	0,1049	> 0	Rejeitar	0,4003	> 0	Rejeitar
4	0,2000	> 0	Rejeitar	0,3705	> 0	Rejeitar
5	0,1671	> 0	Rejeitar	0,4629	< 0	Rejeitar
6	0,2057	> 0	Rejeitar	0,1975	< 0	Rejeitar
7	0,3168	> 0	Rejeitar	0,1284	> 0	Rejeitar
8	0,4336	> 0	Rejeitar	0,4710	> 0	Rejeitar
9	0,4543	> 0	Rejeitar	0,0095	< 0	Não rejeitar ***
10	0,4834	> 0	Rejeitar	0,0229	< 0	Não rejeitar **
11	0,1053	> 0	Rejeitar	0,2835	> 0	Rejeitar
12	0,3788	> 0	Rejeitar	0,1748	< 0	Rejeitar
13	0,0904	< 0	Não rejeitar *	0,2322	> 0	Rejeitar
14	0,2533	> 0	Rejeitar	0,0519	< 0	Não rejeitar *
15	0,2714	> 0	Rejeitar	0,2650	< 0	Rejeitar
16	0,0673	< 0	Não rejeitar *	0,2051	< 0	Rejeitar

	Conhecimento vs Sem Conhecimento			Interesse vs Sem interesse		
Questão	**P Value**	**Relação**	**Conclusão**	**P Value**	**Relação**	**Conclusão**
1	0,0952	< 0	Não rejeitar *	0,1874	< 0	Rejeitar
2	0,0157	< 0	Não rejeitar **	0,1839	< 0	Rejeitar
3	0,4794	< 0	Rejeitar	0,0674	< 0	Não rejeitar *
4	0,2469	> 0	Rejeitar	0,4270	> 0	Rejeitar
5	0,2646	> 0	Rejeitar	0,4416	< 0	Rejeitar
6	0,4802	> 0	Rejeitar	0,2149	< 0	Rejeitar
7	0,0709	> 0	Não rejeitar *	0,2919	< 0	Rejeitar
8	0,4871	< 0	Rejeitar	0,0008	< 0	Não rejeitar ***
9	0,1878	> 0	Rejeitar	0,0562	< 0	Não rejeitar *
10	0,2368	> 0	Rejeitar	0,0778	< 0	Não rejeitar *
11	0,1203	> 0	Rejeitar	0,0661	< 0	Não rejeitar *
12	0,3884	< 0	Rejeitar	0,1685	< 0	Rejeitar
13	0,4049	< 0	Rejeitar	0,1019	< 0	Rejeitar
14	0,4970	> 0	Rejeitar	0,0233	< 0	Não rejeitar **
15	0,0753	< 0	Não rejeitar *	0,1379	< 0	Rejeitar
16	0,2263	> 0	Rejeitar	0,0361	< 0	Não rejeitar **

	Oportunidade vs Sem Oportunidade			Perspetiva vs Sem Perspetiva		
Questão	**P Value**	**Relação**	**Conclusão**	**P Value**	**Relação**	**Conclusão**
1	0,2002	> 0	Rejeitar	0,2115	< 0	Rejeitar
2	0,3711	> 0	Rejeitar	0,4072	< 0	Rejeitar
3	0,1159	> 0	Rejeitar	0,3305	< 0	Rejeitar
4	0,1164	> 0	Rejeitar	0,3510	> 0	Rejeitar
5	0,4629	< 0	Rejeitar	0,3016	> 0	Rejeitar
6	0,3485	> 0	Rejeitar	0,0578	< 0	Não rejeitar *
7	0,4567	< 0	Rejeitar	0,1667	> 0	Rejeitar
8	0,0841	> 0	Não rejeitar *	0,2717	< 0	Rejeitar
9	0,0683	> 0	Não rejeitar *	0,4140	> 0	Rejeitar
10	0,2746	> 0	Rejeitar	0,2678	> 0	Rejeitar
11	0,2835	> 0	Rejeitar	0,2864	< 0	Rejeitar
12	0,3231	> 0	Rejeitar	0,3903	> 0	Rejeitar
13	0,4353	< 0	Rejeitar	0,2410	> 0	Rejeitar
14	0,0507	> 0	Não rejeitar *	0,4680	< 0	Rejeitar
15	0,4361	< 0	Rejeitar	0,0033	< 0	Não rejeitar ***
16	0,3798	> 0	Rejeitar	0,0627	< 0	Não rejeitar *

Apêndice F: Resumo dos Resultados dos Testes *t*

	Eficiência da Auditoria	Qualidade da Auditoria	Auditoria em tempo real	Alteração nas normas de auditoria	Honorários de Auditoria	Intervenção de entidades reguladoras	Concentração do mercado	Maior confiança nos controlos
Atividade vs Sem atividade	SR	SR	SR	SR	SR	SR	SR	SR
Big4 vs Outros	SR	SR	SR	SR	SR	SR	SR	SR
Conhecimento do tema vs Sem conhecimento do tema	Relação *	Relação **	SR	SR	SR	SR	Relação *	SR
Interesse pelo tema vs Sem interesse pelo tema	SR	SR	Relação *	SR	SR	SR	SR	Relação ***
Oportunidades de negócio vs Sem oportunidades de negócio	SR	SR	SR	SR	SR	SR	SR	Relação *
Expetativas futuras vs Sem expetativas futuras	SR	SR	SR	SR	SR	Relação *	SR	SR

Legenda:

SR – Sem relação

Relação * – Existe relação

Relação ** – Existe relação forte

Relação *** – Existe relação muito forte

	Maior recurso a TI	Maior recurso a especialistas	Maior necessidade de confiar em organizações serviços	Menor recurso a amostragem	Menor recurso a confirmações externas	Maior distribuição de procedimentos ao longo do ano	Preparação dos auditores	Apoio dos reguladores
Atividade vs Sem atividade	SR	Relação **	SR	SR	Relação *	SR	SR	Relação *
Big4 vs Outros	SR	Relação **	SR	SR	SR	Relação *	SR	SR
Conhecimento do tema vs Sem conhecimento do tema	SR	SR	SR	SR	SR	SR	Relação *	SR
Interesse pelo tema vs Sem interesse pelo tema	Relação *	Relação *	Relação *	SR	Relação *	Relação **	SR	Relação **
Oportunidades de negócio vs Sem oportunidades de negócio	Relação *	SR	SR	SR	SR	Relação *	SR	SR
Expetativas futuras vs Sem expetativas futuras	SR	SR	SR	SR	SR	SR	Relação ***	Relação *

Legenda:

SR – Sem relação

Relação * – Existe relação

Relação ** – Existe relação forte

Relação *** – Existe relação muito forte