INSTITUTO SUPERIOR DE ENGENHARIA DO PORTO
MESTRADO EM ENGENHARIA ELECTROTÉCNICA E DE COMPUTADORES

# Uma Visão sobre a Tecnologia Blockchain: Domínios de Aplicação e Especificidades na Cadeia de Abastecimento

**EDGAR EMANUEL LEITÃO TAVEIRA**
Outubro de 2020

POLITÉCNICO
DO PORTO


# UMA VISÃO SOBRE A TECNOLOGIA BLOCKCHAIN: DOMÍNIOS DE APLICAÇÃO E ESPECIFICIDADES NA CADEIA DE ABASTECIMENTO

Edgar Emanuel Leitão Taveira

Departamento de Engenharia Eletrotécnica

Mestrado em Engenharia Eletrotécnica e de Computadores

Área de Especialização em Sistemas e Planeamento Industrial

Relatório elaborado para satisfação parcial dos requisitos da Unidade Curricular de Tese/Dissertação do Mestrado em Engenharia Eletrotécnica e de Computadores

Candidato: Edgar Emanuel Leitão Taveira, Nº 1110712, 1110712@isep.ipp.pt
Orientação científica: Professor Filipe Azevedo, fta@isep.ipp.pt


Departamento de Engenharia Eletrotécnica

Mestrado em Engenharia Eletrotécnica e de Computadores

Área de Especialização em Sistemas e Planeamento Industrial

**2020**

*Gostava que aqui estivesses para me ver...*

# *Agradecimentos*

Quero agradecer ao meu orientador, Filipe Azevedo, pelo apoio dado em momentos crucias do desenvolvimento da dissertação. Agradecer a paciência e motivação dada durante o percurso académico conjunto. A forma de ser e de estar cativaram desde a primeira aula.

Agradeço ao Instituto Superior de Engenharia do Porto (ISEP), por ter proporcionado excelentes oportunidades de aprendizagem ricas em conteúdo. Esta, que foi a minha segunda casa durante os últimos anos, ajudou ao meu crescimento pessoal e académico.

Quero deixar um agradecimento ao meu colega de trabalho e amigo, António Maio, por todo o apoio, compreensão e motivação ao longo deste período académico. Não só na escrita da dissertação, mas ainda antes, o apoio fez-se sentir.

Por fim, um agradecimento muito especial à minha mulher, Catarina Ciríaco, pelo carinho, compreensão e motivação que foi dando ao longo deste meu percurso e prossecução de objetivo académico. Várias foram as horas que o dever académico se sobrepôs ao dever familiar. Agradeço toda a compreensão e força dadas em alturas de dúvida.

# *Resumo*

A tecnologia *blockchain* tem assumido um papel de destaque no mundo tecnológico. Assistimos ao aparecimento do conceito de indústria 4.0, que pretende a transferência de autonomia para as máquinas. Esta autonomia só é possível de atingir através de uma grande quantidade de dados e transações adquiridos através de sensores ou outros dispositivos ligados entre si – Internet das Coisas. A necessidade de uma taxa grande de transações e de passagem de informação confiável e fidedigna, entre atores pertencentes a uma mesma rede confiável, leva ao aparecimento da tecnologia *blockchain* em 2008, com a *Bitcoin*. Anos antes, a ideia de cadeias de blocos criptograficamente protegidas, já havia sido desenvolvida, embora com limitações na forma de gerar consenso entre os diferentes agentes. Desde 2008, têm sido desenvolvidos diferentes algoritmos de consenso para uma rede *blockchain*. Desde o original *proof-of-work*, passando pelo *proof-of-stake* até a métodos de *directed acyclic grap*h, a forma como o consenso é gerado numa rede *blockchain* digitalmente imutável assume diferentes formas, com diferentes benefícios e limitações. O objetivo desta dissertação é estudar a tecnologia *blockchain* e os seus avanços tecnológicos, garantindo uma visão geral da mesma. Com base no seu funcionamento, identificar domínios de aplicação desta tecnologia, com especial enfoque na cadeia de abastecimento e área logística, devido ao seu potencial de benefícios a atingir. É igualmente pretendido, uma abordagem às limitações e requisitos necessários para a sua aplicação em ambiente produtivo, uma vez que, nesta área as aplicações ainda não se encontram em fases avançadas.

# *Palavras-Chave*

*blockchain*, indústria 4.0, internet das coisas, cadeia de abastecimento, logística

# *Abstract*

Blockchain technology has assumed a prominent role in the technological world. We have seen the emergence of the concept of industry 4.0, which aims to transfer autonomy to machines. This autonomy is only possible to achieve through a large amount of data and transactions acquired through sensors or other connected devices - the Internet of Things. The need for a high rate of transactions and the passing of reliable and trustworthy information between actors belonging to the same trusted network, leads to the appearance of blockchain technology in 2008, with Bitcoin. Years earlier, the idea of cryptographically protected blockchains had already been developed, albeit with limitations on how to generate consensus between different agents. Since 2008, different consensus algorithms have developed for a blockchain network. From the original proof-of-work, through the proof-of-stake to methods as directed acyclic graph, the way consensus is generated in a digitally immutable blockchain network takes different forms, with several benefits and limitations. The purpose of this dissertation is to study blockchain technology and its technological advances, ensuring an overview of it. Based on its operation, identify areas of application of this technology, with a particular focus on the supply chain and logistics area, due to its potential benefits to be achieved. It is intended, an approach to the limitations and requirements necessary for its application in a production environment, since, in this area, applications are not yet in advanced stages.



# *Keywords*

Blockchain, industry 4.0, Internet of Things, supply chain, logistics

# *Índice*

# *Índice de Figuras*

# *Índice de Tabelas*

# *Lista de Siglas e Abreviaturas*

P2P – *Peer-to-Peer*

I4.0 – Indústria 4.0

IoT – *Internet-of-Things*

DLT – *Distributed Ledger Technology*

nonce – *Number only used once*

PoW – *Proof-of-Work*

PoS – *Proof-of-Stake*

BFT – *Byzantine Fault Tolerance*

SC – *Smart Contracts*

PoA – *Proof-of-Activity*

PoB – *Proof-of-Burn*

PoC – *Proof-of-Capacity*

PoET – *Proof-of-Elapsed-Time*

DAG – *Direct Acyclic Graph*

PBFT – *Practical Byzantine Fault Tolerance*

FBA – *Federated Byzantine Agreement*

DBFT – *Delegated Byzantine Fault Tolerance*

SCM – *Supply Chain Management*

RFID – *Radio-Frequency Identification*

API – *Application Programming Interface*

REST – *Representational State Transfer*

HTTP – *Hypertext Transfer Protocol*

JSON – *JavaScript Object Notation*

ETH – *Ether*

# 1. INTRODUÇÃO

Este projeto surgiu do desejo de realizar um trabalho no âmbito da tecnologia *blockchain*. O interesse nas especificidades de aplicação da tecnologia à cadeia de abastecimento (*supply chain*) surge nos desafios inerentes encontrados dentro desta área que, apresenta de igual forma, um enorme potencial de benefícios com a tecnologia.

Apesar de a tecnologia *blockchain* estar enraizada na associação às criptomoedas, sendo a *Bitcoin* um dos (muitos) exemplos [1], esta tecnologia tem potencial para outras aplicações avançadas [2][3]. Sendo uma tecnologia considerada das mais disruptivas atualmente, permite a criação de soluções descentralizadas, a execução autónoma de contratos e o controlo de ativos através da internet [4].

A escolha do tema nesta dissertação pretende estudar a tecnologia *blockchain* de outra maneira, analisando de que forma esta tecnologia poderá afetar as empresas e fábricas na sua cadeia de abastecimento. Em suma, o objetivo é olhar a tecnologia como uma alternativa ao atual mecanismo de controlo e rastreamento da cadeia de abastecimento de uma empresa ou fábrica.

## 1.1. CONTEXTUALIZAÇÃO

Devido à complexidade e falta de transparência entre todos os agentes ativos de uma cadeia de abastecimento (*supply chain*) tradicional, surge o interesse na investigação da aplicação da tecnologia *blockchain* no ambiente logístico [5]. Esta tecnologia promete melhorar os processos logísticos, assim como aumentar a sustentabilidade da rede de agentes ativos na cadeia de abastecimento (*supply chain*) [5][6].

Numa cadeia de abastecimento tradicional (*supply chain*), a informação é armazenada centralmente [6]. Este facto torna a informação suscetível a ataques maliciosos ou à perda de informação devido a erros ou problemas com o fornecedor de serviços [6]. A tecnologia *blockchain* mostra potencial no aumento da segurança e privacidade dos dados e

informação armazenada [6], uma vez que cada bloco de informação constituinte da rede está diretamente ligado ao anterior e ao seguinte [2][3]. Por este motivo, a tecnologia *blockchain* permite um rastreamento mais seguro de qualquer tipo de transação gerada, sendo possível reduzir custos relacionados com atrasos de informação, erro humano ou qualquer custo adicional referente à perda de dados [6].

A *blockchain* pode ser explicada como um livro de registos descentralizado (na literatura anglo-saxónica, *ledger*) [7]. Este *ledger* descentralizado apresenta diversas aplicações no que diz respeito a tratamento e armazenamento de diferentes tipos de registo e transações, devido ao seu modo de funcionamento.

Originalmente desenvolvida no seio das criptomoedas com a criação da *Bitcoin* [8][9], a *blockchain* funciona com uma estrutura de dados distribuída com base em transações de rede ponto a ponto (*peer-to-peer, P2P*) [9][10][11]. Todos os blocos da rede estão ligados entre si através de uma *hash* criptográfica [9][12], onde cada nó (na literatura anglo-saxónica, *peer*) da rede possui uma cópia da informação presente em toda a *blockchain* [9][13][14]. Estas características tornam os registos e transações da rede virtualmente imutáveis [9][15][16][17].

Os atributos da tecnologia *blockchain* oferecem mais segurança [18], e a imutabilidade dos registos ordenados de forma cronológica oferece uma melhor rastreabilidade da informação [18]. É por estas razões que se crê que esta tecnologia possa aumentar a eficiência e a transparência da cadeia de abastecimento (*supply chain*) e afetar de forma positiva todos os processos logísticos [6][7].

## 1.2. OBJETIVOS DA DISSERTAÇÃO

O âmbito deste trabalho é estudar de que forma a tecnologia *blockchain* será capaz de influenciar a cadeia de abastecimento (*supply chain*) e área logística das empresas, analisando a viabilidade da aplicação de tecnologia *blockchain* no âmbito da *supply chain* e quais os possíveis benefícios e/ou lacunas existentes nesta tecnologia e aplicação.

De modo a melhor orientar a investigação do tema, foram desenvolvidos dois objetivos específicos [19][20] que têm o propósito de servir como alicerces teóricos à execução do trabalho e, de igual forma, garantir um entendimento claro do tema estudado.

- Objetivo 1: De que forma a tecnologia *blockchain* está relacionada com a cadeia de abastecimento (*supply chain*) e logística?
- Objetivo 2: Qual *blockchain ledger* é mais adequado para aplicações na área de cadeia de abastecimento (*supply chain*) e logística?

No primeiro objetivo, o propósito é entender de que forma a tecnologia pode ou não estar relacionada com a cadeia de abastecimento (*supply chain*) e área logística. A intenção é entender junto da literatura científica, de que forma podemos olhar para estes dois tópicos (*blockchain* e *supply chain*).

No segundo objetivo, o propósito consiste em perceber quais as diferentes aplicações que a *blockchain* pode ter e quais os *ledgers* mais indicados para a mesma.

## 1.3. METODOLOGIA DE INVESTIGAÇÃO

A base de dados para a revisão de literatura foi a *SCOPUS* [21][22]. Foi desenvolvido inicialmente uma *query* de pesquisa assente nos módulos da Tabela 1. O objetivo da pesquisa foi encontrar revisões de literatura atuais relativas ao tema da blockchain, com especificidades assentes na cadeia de abastecimento. A pesquisa na *SCOPUS* retornou 42 documentos. Estes documentos foram analisados e incluídos na escrita deste capítulo. Quando pertinente, foram analisados artigos adjacentes aos inicialmente selecionados.

A *query* final utilizada foi:

- *TITLE-ABS-KEY ( blockchain AND ( "Supply Chain" OR "Logi*" ) AND ( "Systematic Literature Review" OR "Systematic Review" OR "Review" OR "Literature Review" ) ) AND ( LIMIT-TO ( SRCTYPE , "j" ) )*

**Tabela 1** - Criação de *query* para SCOPUS

| | | |
|---|---|---|
| População | "*Blockchain*" | Área de estudo principal |
| Contexto 1 | *AND ( "Supply Chain" OR "Logi*" )* | Área de estudo secundária<br>"***Supply Chain***" e "***Logistics***" |
| Contexto 2 | *AND ( "Systematic Literature Review" OR "Systematic Review" OR "Review" OR "Literature Review" ) )* | Área de estudo relacional<br>"***Systematic Leterature Review***" |
| Filtro 1 | *AND ( LIMIT-TO ( SRCTYPE , "j" ) )* | Limitar a publicações em "***Journals***" |

Para além dos artigos científicos derivados da SCOPUS, o estudo foi complementado com pesquisa na *web*. De forma a garantir uma boa gestão de referências bibliográficas, foi utilizado o *Mendeley* [23][24].

## 1.4. ESTRUTURA DA DISSERTAÇÃO

A dissertação está dividida em cinco capítulos. O primeiro capítulo apresenta a "Introdução" da dissertação com a devida contextualização, exposição dos objetivos e apresentação da metodologia utilizada para o tratamento, pesquisa e desenvolvimento teórico da componente científica da dissertação apresentada. O capítulo dois explica a tecnologia *blockchain* e os diferentes tipos de consenso da mesma. No terceiro capítulo são abordados os *Smart Contracts* e os domínios onde a tecnologia *blockchain* pode ter impacto, para além das criptomoedas. O capítulo quatro foca as especificidades da cadeia de abastecimento e a relação com a tecnologia *blockchain*, culminando numa síntese de três *ledgers* utilizados nesta área de aplicação. O quinto capítulo implementa uma *blockchain* simples com recurso ao *ledger Hyperledger Fabric* e exemplifica algumas funcionalidades através do *Docker* e *Smart Contracts*. O sexto e último capítulo apresenta

as conclusões do trabalho realizado, sugestões de trabalho futuro e aborda algumas limitações do corrente trabalho apresentado.

# 2. A TECNOLOGIA BLOCKCHAIN

Este capítulo aborda o tema "Indústria 4.0" de forma a categorizar a área abrangente onde a tecnologia *blockchain* está inserida. É desenvolvido o tema "Tecnologia *blockchain*" como um todo, passando por referências históricas até ao funcionamento base de uma *blockchain*. Após a componente conceptual, são abordados os diferentes mecanismos de *consensus* numa *blockchain*.

## 2.1. INDÚSTRIA 4.0

Desenvolvimentos tecnológicos em larga escala têm sido introduzidos diretamente na indústria, originando uma nova abordagem intitulada "Indústria 4.0" (i4.0) [25][26]. Este conceito, i4.0, pretende combinar vários domínios tecnológicos de modo a melhorar processos e resultados industriais [25]. Alguns exemplos de domínios tecnológicos são, entre outros, a internet das coisas (ou "*Internet-of-Things*" (IoT)), a tecnologia *blockchain* e outros sistemas ciberfísicos (CPS) [25][26].

O conceito de i4.0 é holístico, propondo uma transferência de autonomia, inteligência e tomada de decisão para as máquinas [6][27]. Estas características permitem a otimização de processos logísticos, garantindo a integração e alinhamento com os limites corporativos das empresas [27]. Quando a aplicação deste conceito é bem-sucedida, muitos dos problemas logísticos relacionados com os fluxos de entrada e saída de materiais podem ser significativamente simplificados [6][27].

De modo a potenciar a aplicação no domínio i4.0, é necessário aplicar uma abordagem de *big data* [6][28]. O termo "*big data*" abrange o grande volume de dados estruturados e não estruturados, que cresce exponencialmente usando análise de dados e armazenamento [6][28].

Estas características adjacentes à indústria 4.0 levam as empresas a digitalizar e automatizar os seus processos na procura de melhorias e aumento de lucro [25]. No entanto, ao adicionar agentes autónomos aos processos, aumentam os custos de transações e o risco das mesmas [25]. O risco está intrinsecamente ligado à confiança dos agentes e à sua comunicação centralizada [25]. Para adereçar estes riscos, começam a existir estudos sobre o uso de soluções descentralizadas (como a tecnologia *blockchain*) para melhorar a eficiência e segurança na comunicação entre os agentes autónomos num sistema multiagente [29][30].

### 2.1.1. A INTERNET DAS COISAS

Estima-se que o número de dispositivos habilitados para IoT atinga o valor de 24 biliões no ano 2020 [31]. Este facto, envolve uma enorme criação de informação que necessita de ser transacionada e armazenada de forma segura e eficiente [25]. A internet das coisas (IoT), consiste numa rede com múltiplos dispositivos capazes de interagirem entre si através de qualquer canal aberto, como a *internet* [32][33]. Esta capacidade de interação autónoma e o crescimento nos sistemas baseados em IoT no âmbito da i4.0, geram a necessidade de uma tecnologia capaz de processar e suportar esta quantidade de dados crescente de uma forma eficiente e segura [25].

Atualmente, a maioria dos sistemas IoT são baseados em soluções centralizadas [34][35]. Este aspeto da arquitetura centralizada de sistemas IoT para o desenvolvimento da indústria 4.0 (i4.0), apresenta duas limitações importantes [36]:

1. A presença de um único ponto de falha;
2. Falta de confiança entre as partes integrantes do sistema.

De modo a colmatar as limitações apresentadas, é possível utilizar soluções descentralizadas para comunicação ponto-a-ponto (*peer-to-peer*) entre os diferentes dispositivos do sistema [25]. Os sistemas descentralizados baseados na tecnologia *blockchain*, são uma possível solução [25].

Uma das vantagens do uso da *blockchain* é poder garantir a imutabilidade dos dados, sem depender de uma solução centralizada de armazenamento [25]. A sua encriptação dá uma

garantia de segurança em todas as transações efetuadas na rede e permite um registo cronológico das mesmas [25].

A tecnologia *blockchain* pode ajudar a potenciar o uso de sistemas IoT no âmbito i4.0 com uma plataforma aberta, confiável, segura e auditável [25]. Alguns dos benefícios da integração de *blockchain* no âmbito da indústria 4.0 e sistemas IoT, são [37][38][39]:

- Descentralização e escalabilidade – Eliminando a limitação de um único ponto de falha em comparação com uma solução centralizada, é capaz de aumentar a tolerância a falhas;
- Identidade – A imutabilidade subjacente a esta solução permite uma melhor rastreabilidade da informação, aumentando a segurança na autenticação de agentes e dispositivos presentes na rede;
- Autonomia – O uso de soluções descentralizadas garante uma maior autonomia aos agentes e dispositivos da rede, permitindo a eliminação de pontos intermédios. Desta forma, os dispositivos podem comunicar diretamente entre si, não precisando de um intermediário para que a comunicação aconteça ou para que a transação seja validada;
- Segurança – Com o recurso a *smart contracts*, é possível que a troca de informação seja tratada como uma transação, o que permite uma comunicação segura entre dispositivos e agentes devido à encriptação da rede;
- Fiabilidade – No uso de tecnologia *blockchain*, é possível validar a autenticidade de cada transação assim como o responsável pela mesma.

Estas características da tecnologia *blockchain*, tornam esta solução descentralizada uma opção na integração de sistemas IoT para o desenvolvimento do conceito i4.0 [25].

## 2.2. TECNOLOGIA BLOCKCHAIN

A tecnologia *blockchain* consiste num sistema descentralizado. Vários agentes, ou nós (*nodes, ou peers*), constituem este sistema descentralizado, trabalhando em conjunto dentro da rede *blockchain* [1]. Cada nó está indiretamente conectado a outro sem nunca estarem diretamente ligados a todos os nós constituintes da rede *blockchain* [1].

Este *modus operandi* contrasta com os sistemas centralizados, onde todos os agentes de uma rede estão diretamente conectados a um nó central [1], conforme exemplificado na Figura 1 [40]. Por esta razão, os sistemas descentralizados começam a ganhar preferência sobre sistemas centralizados, devido ao processamento mais rápido, custo de manutenção reduzido, maior estabilidade de sistema e processos de atualização mais fáceis [41].

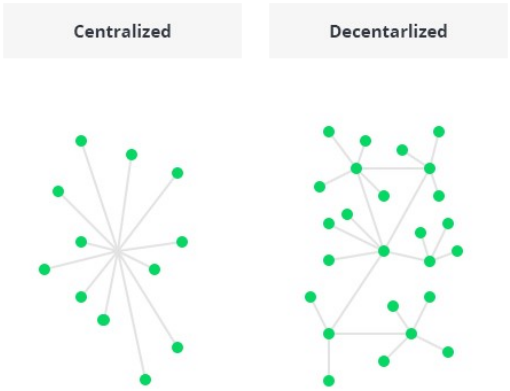


**Figura 1** Sistemas centralizados vs. Sistemas descentralizados [40]

Ao longo do tempo, podemos identificar três momentos chave na evolução e desenvolvimento da tecnologia *blockchain* [42][43]. O primeiro momento-chave consiste na aplicação da tecnologia *blockchain* no âmbito das criptomoedas (*Blockchain* 1.0). O segundo momento-chave introduz a criação de *smart contracts* e algumas aplicações fora do ambiente financeiro das criptomoedas (*Blockchain* 2.0). O terceiro, e atual, momento em que a tecnologia *blockchain* se encontra (*Blockchain* 3.0), consiste na aplicação em áreas e domínios como a saúde, política, ciência e IoT, abrangendo a "revolução" da indústria 4.0 (i4.0) [42][43].

### 2.2.1. CONTEXTO HISTÓRICO

A base da tecnologia *blockchain* remonta a 1991 [6]. Neste ano foi publicado um trabalho no domínio de cadeias de blocos criptograficamente protegidas [44]. No par de anos seguinte, os mesmos autores introduziram árvores de dispersão, ou árvores de *Merkle* (na literatura anglo-saxónica, *Merkle Trees*), o que permitiu um avanço na quantidade de

informação armazenada por bloco [45]. Em 2008 a tecnologia *blockchain* surge com o trabalho apresentado pelo pseudónimo *Satoshi Nakamoto* sobre a *Bitcoin* [6][8].

A primeira *blockchain* desenvolvida foi aplicada no setor financeiro, onde serviu de base à criptomoeda *Bitcoin* [8]. Esta criptomoeda, dotada de tecnologia *blockchain*, é baseada num sistema ponto a ponto (*peer-to-peer* ou P2P) onde opera sem qualquer autoridade intermediária confiável, como um banco, um revisor oficial de contas, um notário ou qualquer outro serviço centralizado [6].

A revolução que a *Bitcoin* originou no steor tecnológico financeiro (na literatura anglo-saxónica, *Fintech*), afeta igualmente todos os tipos de indústria e não só instituições financeiras [1]. O desenvolvimento de um arquivo digital distribuído, ou *distributed ledger technology* (DLT), tornou a tecnologia *blockchain* atrativa para múltiplas indústrias, incluindo o setor industrial e de manufatura [41][46]. Um dos fatores deve-se à DLT ser partilhada por todos os intervenientes do sistema, aumentando assim a transparência da informação em tempo real [41][46].

### 2.2.2. FUNCIONAMENTO DA BLOCKCHAIN

*Blockchain* é um sistema descentralizado, verificável e imutável [47]. Uma arquitetura descentralizada, ou distribuída, significa que o sistema não depende de uma autoridade central [48]. Ao invés, utiliza uma rede ponto a ponto (*peer-to-peer* ou P2P) de agentes, mantida por proprietários descentralizados [48]. Nesta rede, todos os pontos/nós possuem uma cópia da *blockchain* [48]. No entanto, a segurança é conseguida através do uso de criptografia de chave público-privada em cada transação [49]. Qualquer tentativa de adulterar transações ou a própria rede é notificada pelos diversos pontos/nós pertencentes à rede [49]. Desta forma, a *blockchain* garante a imutabilidade das transações e, por conseguinte, a verificabilidade da informação [48][49]. A informação armazenada neste *distributed ledger* está ordenada de forma sequencial e cronológica, guardando o *timestamp* de criação do bloco (transação), a *hash* criptográfica do bloco anterior e os detalhes da transação [9][50][51].

Faz mais de uma década desde que *Satoshi Nakamoto* descreveu a tecnologia *Blockchain* como uma estrutura *peer-to-peer* (P2P) distribuída, capaz de manter a ordem dos registos e transações, assim como resolver o problema de *double spending* [8][52]. A questão do *double spending* foi o calcanhar de Aquiles na primeira tentativa de criar uma cripto-moeda, a *Bit Gold* em 2005 por *Nick Szabo* [53]. Esta questão prende-se com o facto de garantir que, digitalmente, não é possível utilizar a mesma quantia duas vezes. Com o uso de dinheiro físico este problema não acontece. Igualmente, no Mundo real, existem as instituições financeiras que atuam como intermediários e, por isso, regulam as transações feitas garantindo a mitigação e resolução deste problema [54]. As criptomoedas funcionam de forma diferente. Cada transação efetuada é transmitida a todos os pontos/nós da rede, que têm de validar e confirmar a transação. Este processo consome tempo e o problema de *double spending* acontece aqui - o que impede alguém de copiar uma transação e retransmiti-la antes de ser confirmada na rede? [54][55][56]

A *Bitcoin* organiza transações e agrupa-as numa estrutura de tamanho restrito – bloco – partilhando o registo de data e hora – *timestamp* [42][57]. Os nós da rede – *miners* – são responsáveis por ligar os blocos entre si por ordem cronológica [42][57]. Cada bloco contém o código criptográfico – *hash* – do bloco anterior para criar um arquivo de transações/blocos ordenado – *ledger* [42][57]. A Figura 2 mostra o funcionamento da *Bitcoin* [58].

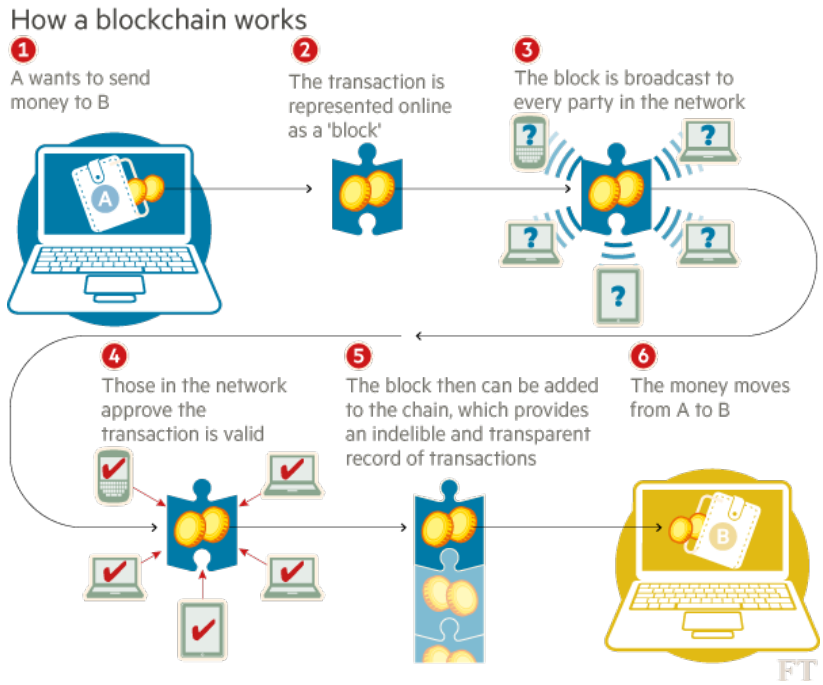


**Figura 2** Funcionamento da *Bitcoin* [58]

O termo *blockchain* é amplamente associado às criptomoedas como a *Bitcoin* [8], *Ethereum* [59] ou *Ripple* [60][61]. No entanto, é de notar que as criptomoedas são um resultado possível do uso da tecnologia *blockchain*, uma vez que a *blockchain* pode existir sem qualquer tipo de cripto-moeda [62].

*Blockchain* é definida da seguinte forma: "é uma base de dados distribuída, partilhada e agrupada numa rede *peer-to-peer*. Consiste numa sequência ligada de blocos, onde são mantidas transações com registo de data e hora, protegidas por criptografia de chave assimétrica e verificadas pela comunidade da rede. Depois de um bloco ser agregado à *blockchain*, não pode ser alterado, transformando uma *blockchain* num registo imutável de atividades passadas" [6][27][63].

O funcionamento da *blockchain* pode ser descrito analisando a forma como uma transação é incorporada na *blockchain*. Na Figura 3 podemos ver uma explicação genérica da criação de blocos numa *blockchain* [64].

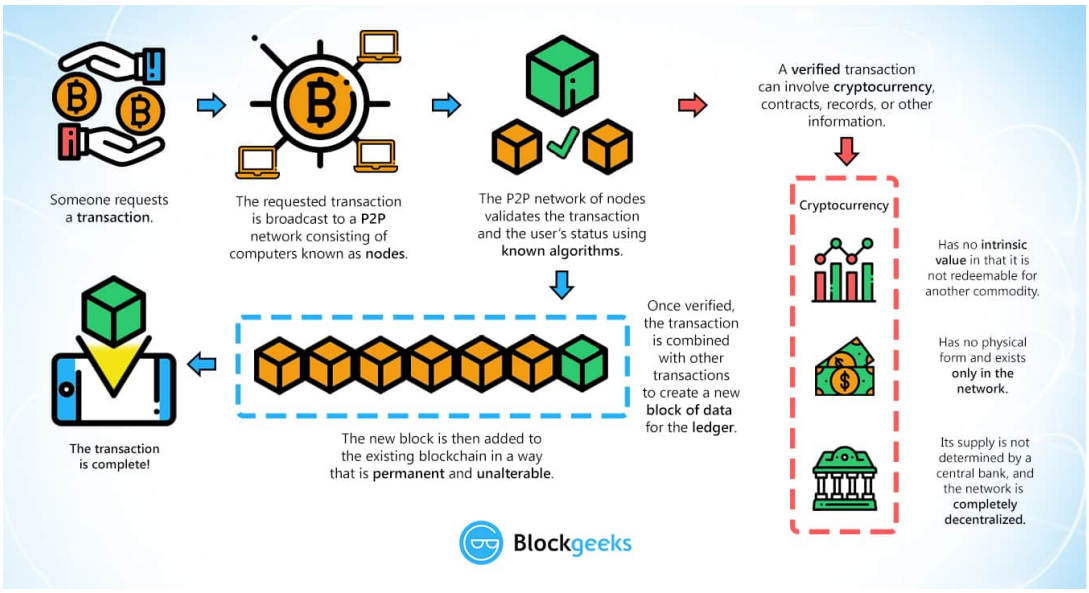


**Figura 3** Esquema do funcionamento da *blockchain* [64]

Quando é iniciado um pedido de transação na rede distribuída *peer-to-peer* (P2P) – chamada *blockchain* – é necessário que o utilizador que iniciou o pedido forneça uma prova de identidade à rede. Esta prova de identidade tem como base a criptografia de chave público-privada, ou criptografia assimétrica, e serve para fazer prova de que o utilizador é quem afirma ser dentro da rede [58][65].

Os detalhes da transação são guardados num bloco. Este bloco é transmitido a todos os pontos/nós da rede P2P para que estes possam verificar e validar a transação. Os pontos/nós constituintes da rede trabalham em conjunto para validar a transação – resolvendo problemas matemáticos computacionais. Ao processo de validação de transações, dá-se o nome de *mining* [52][58][65][66].

Por ser uma rede distribuída e descentralizada, cada ponto/nó da rede guarda uma cópia de todos os blocos previamente validados – algo semelhante a uma corrente de blocos ou um arquivo em constante atualização [58] (daí os termos *blockchain* e *ledger*).

Assim que um ponto/nó da rede resolve o algoritmo de validação, a transação é verificada e o novo bloco é adicionado à *blockchain* pelo nó que resolveu o problema. Após a introdução do novo bloco na *blockchain*, o nó que o adicionou transmite à rede que um novo conjunto de informação foi adicionado ao arquivo de transações [58].

Após a transmissão, todos os pontos/nós da rede verificam o novo bloco e, através do algoritmo de validação da *blockchain*, validam a legitimidade da transação (*distributed consensus*) [65][66][52]. Quando o consenso é atingido, todos os pontos/nós da rede atualizam a sua cópia do arquivo de transações – *blockchain ledger* [58].

A forma como as transações são criadas, verificadas, armazenadas e validadas, torna a *blockchain* num registo de transações imutável, transparente e indelével. Qualquer tentativa para adulterar o sistema é notada aquando a prova de identidade necessária para escrita na rede. Caso haja tentativas de adulteração, todos os pontos/nós da rede são alertados e, por isso, a adulteração dos registos falha [52]. Na Figura 4 é exemplificado o registo de transações numa *blockchain* [58].

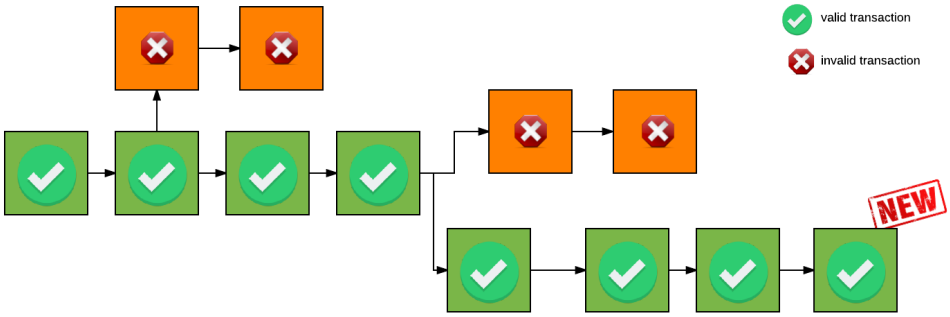


**Figura 4** Registo de transações numa rede *blockchain* [58]

### 2.2.3. CRIPTOGRAFIA APLICADA À BLOCKCHAIN

A tecnologia *blockchain* é baseada num método no qual partes anteriormente desconhecidas podem gerar e manter em conjunto qualquer base de dados de uma forma totalmente distribuída, onde a integridade das transações é validada usando algoritmos de consenso entre as diferentes partes independentes [6][44]. Esta forma de funcionamento, anteriormente explicada no ponto 2.3.2., utiliza a ciência da criptografia de modo a conseguir o ambiente confiável associado à tecnologia *blockchain* [61].

No momento da criação de uma transação, é necessário que o utilizador faça prova da sua identidade. A prova criptográfica de identidade significa, simplesmente, provar a identidade de alguém sem a revelar publicamente [58]. Para que esta prova de identidade aconteça, é necessária a criação de uma assinatura digital integrada com criptografia assimétrica de modo a garantir a premissa do anonimato confiável e verificável [67].

Uma assinatura digital, assenta em três pontos-chave [68]:

1. Deve ser verificável – A assinatura digital deve poder verificar que o proprietário é quem afirma ser;
2. Não deve ser copiável – Não deve ser possível a cópia da assinatura digital, sendo esta única;
3. Não pode ser desassociada – Sendo atribuída uma assinatura digital, o proprietário não pode alegar não ser quem é, ou seja, não pode desassociar-se da própria assinatura digital;

O conceito de assinatura digital, está ligado à criptografia moderna [69]. A criptografia é o estudo e desenvolvimento de métodos que, usando princípios matemáticos avançados, conseguem armazenar e transmitir dados de forma segura [70]. Esta segurança está diretamente ligada à criação de protocolos para impedir a leitura de mensagens/transações privadas, garantindo que somente aqueles para quem se destina a mensagem/transação possam ler e processar a informação enviada [69][71]. À transformação da mensagem/transação no momento do envio dá-se o nome de encriptação, ou cifragem, enquanto que à transformação da mensagem/transação no momento da receção dá-se o nome de desencriptação, ou decifragem [72].

Existem, essencialmente, dois domínios da criptografia. Criptografia de chave-privada, ou criptografia simétrica, e criptografia de chave-pública, ou criptografia assimétrica [68][69].

A criptografia de chave-privada, ou criptografia simétrica, é distinguida pelo funcionamento do algoritmo de encriptação, ou cifragem. Neste modelo criptográfico simples, a característica principal é a utilização da mesma chave criptográfica para a encriptação da mensagem/transação e desencriptação da mesma [72]. Com este modelo de encriptação, a chave digital é partilhada com todos os pontos/nós para os quais se queira estabelecer uma ligação. Este protocolo de chave-privada levanta algumas questões referentes à criação dessa mesma chave. Uma vez que esta é partilhada por todos os pontos/nós de comunicação, é colocada em causa a segurança no momento da partilha da chave digital [70][72].

A criptografia de chave-publica, ou criptografia assimétrica, utiliza um par de chaves criptográficas diferentes, embora relacionadas matematicamente entre si. Desta forma, através da primeira chave digital (chave privada), consegue gerar uma segunda chave única e verificável (chave pública), garantindo, através da dificuldade de engenharia reversa, que o contrário não é possível. Através do conhecimento da segunda chave digital (chave pública) não é possível chegar à origem, ou seja, descobrir a primeira chave digital (chave privada) [72]. A característica principal da criptografia assimétrica é a utilização de diferentes chaves nos processos de encriptação e desencriptação da mensagem/transação [69][70].

Um conceito comum aos domínios da criptografia é a função de *hash*, ou *hashing*. Foram apresentados modelos de encriptação que certificam a segurança da mensagem/transação, garantindo que a informação é legível por pontos/nós autorizados. Estes protocolos asseguram igualmente a autenticidade da mensagem/transação através da prova de identidade do par emissor/recetor [70]. No entanto, para garantir que a informação presente na mensagem/transação não é alterada, ou distorcida pelo processo de encriptação, é necessário certificar que a mensagem recebida corresponde integralmente à mensagem enviada [72]. Para assegurar esta conformidade existe a função de *hash*, ou *hashing*.

*Hashing* refere-se ao conceito de, através de um algoritmo ou função de *hash*, representar uma qualquer variável de entrada de uma forma condensada e de tamanho fixo [67]. A esta representação de saída, dá-se o nome de *hash value*, *hash code*, ou simplesmente *hash* [72]. Estas funções são importantes, pois transformam qualquer informação (independentemente do tamanho) numa variável de tamanho fixo. A garantia da veracidade e conformidade da mensagem/transação deve-se ao facto das funções de *hash* serem consideradas funções estatisticamente livres de colisões [69]. Isto significa que quando possuímos duas variáveis diferentes, para efeitos práticos, a probabilidade de produzirem dois *hash values* iguais é nula [72].

Associado ao *hashing*, podemos encontrar o conceito criptográfico de *Merkle Trees* [73]. Este conceito é fundamental no funcionamento de uma *blockchain* [74]. Na Figura 5 é possível ver a estrutura deste conceito.

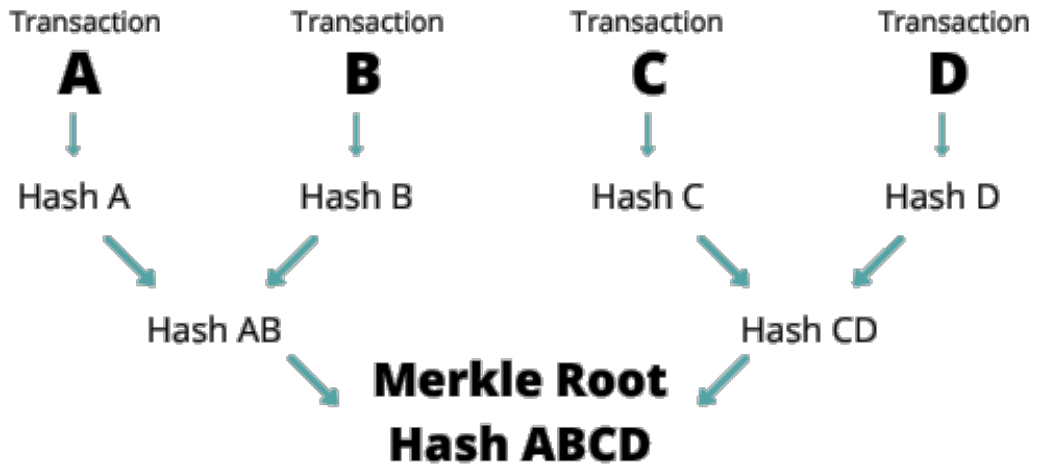


**Figura 5** Estrutura *Merkle Tree* [74]

O código único que uma *Merkle Tree* produz é chamado de *Merkle Root*. Cada bloco individual de uma *blockchain* possui um. O conceito de *Merkle Trees* agrupa todas as entradas de dados em pares. Se houver um número ímpar de entradas, a última entrada é copiada e associada com ela mesma. Isto aplica-se a todos as transações gravadas num bloco de uma *blockchain* [73][74].

Por exemplo, um único bloco contém um total de 424 transações. Este conceito inicia agrupando todas as transações em 212 pares. De seguida é feito o *hashing* originando 212 novos códigos encriptados. O processo repete-se até atingir apenas um único código – *Merkle Root* – ou seja, 212 > 106 > 53(54) > 27(28) > 14 > 7(8) > 4 > 2 > 1. Este será o código associado à informação das transações gravadas nos blocos de uma *blockchain* [74].

Pelo funcionamento das funções de *hash*, aquando a criação de uma mensagem/transação é gerada um *hash value*. No momento da receção, a comparação do *hash value* da mensagem enviada com o *hash value* da mensagem recebida irá determinar se houve algum tipo de perda ou distorção na mensagem/transação [70]. Desta forma, é garantida a integridade da mensagem/transação [72].

A importância da função de *hash* é transportada para o conceito de assinatura digital, introduzido acima. Uma assinatura digital compreende algoritmos de *hashing* e criptografia assimétrica, de forma a gerar uma marca digital que, anexa a uma mensagem/transação,

consiga garantir a autenticidade da informação e, simultaneamente, a identificação da sua autoria [67][71][72].

Num primeiro momento, o ponto/nó que quer enviar uma mensagem/transação, obtém o *hash value* da mensagem/transação que pretende enviar. Após a obtenção do *hash value*, este é encriptado utilizando a chave privada (a primeira chave digital de criptografia assimétrica), originando uma assinatura digital. Esta assinatura é, então, associada à mensagem/transação enviada [67][72].

Do lado do recetor, aquando a receção da mensagem/transação, é possível a descodificação da mesma através da chave pública (a segunda chave digital de criptografia assimétrica). Esta desencriptação permite obter um *hash value* que, quando comparado com o *hash value* da mensagem enviada, permite verificar a autenticidade e integridade da mesma. O facto da chave pública utilizada ter originado um *hash value* igual ao da mensagem enviada, identifica o autor da mensagem [67][72].

É a assinatura digital que é necessária aquando a criação de uma mensagem/transação na *blockchain* [58]. Devido ao uso de criptografia assimétrica, *hashing* e assinatura digital, a tecnologia *blockchain* garante a segurança, autenticidade, integridade, transparência e rastreabilidade das mensagens/transações geradas [68]. A informação fica, então, armazenada em blocos, cada um correspondendo a uma mensagem/transação, ordenados cronologicamente e validados pela rede P2P [25][61].

### 2.2.4. Estrutura de um Bloco de Transações da Blockchain

A *blockchain* é um arquivo de transações – *ledger* – que opera num ambiente confiável e seguro através de criptografia moderna. Conforme explicado no ponto 2.3.3., um conjunto finito de transações é armazenado em blocos protegidos por assinatura digital e funções de *hash* com criptografia assimétrica [61]. De modo a aumentar a segurança da *blockchain*, cada bloco, aquando a sua criação, usa o *hash value* do bloco imediatamente anterior e serve de base para a criação do bloco imediatamente a seguir. Isto é, o bloco seguinte faz exatamente o mesmo, ficando ligado ao anterior e assim sucessivamente. Desta forma é garantida uma "cadeia de blocos" ordenada e de caminho único, com uma estrutura semelhante à ilustrada na Figura 6.

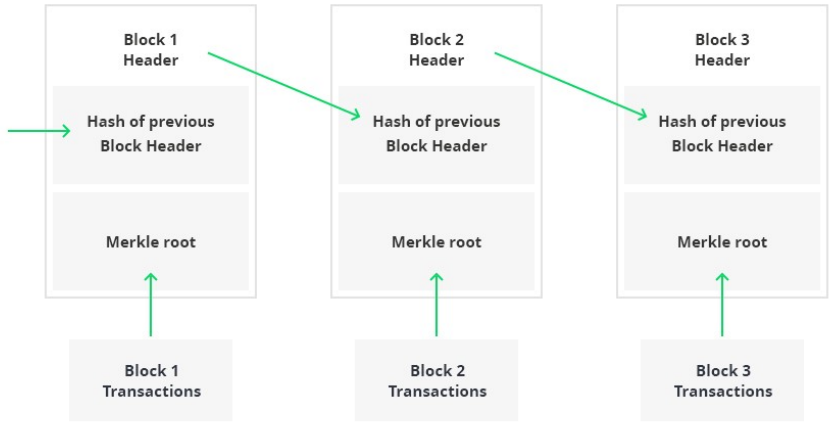


**Figura 6** Estrutura de um bloco [40]

As transações e informações guardadas em cada bloco utilizam o conceito de *Merkle Tree* para um processamento computacional mais rápido. O conceito de *Merkle Tree*, faz o *hash* dos registos presentes no *ledger*, onde separa efetivamente a prova dos dados dos próprios dados. Assim, provar que uma transação é válida envolve apenas o envio de pequenas quantidades de informação pela rede [45][73][74].

A estrutura da tecnologia *blockchain* é representada por uma lista de blocos com transações ordenadas linearmente no tempo. O funcionamento dos blocos assenta em duas estruturas [40]:

- Apontadores (*pointers*) – São variáveis que contêm informação sobre a localização de outra variável;
- Listas de dados ligadas – Uma sequência de blocos, onde cada bloco possui dados específicos e apontadores para o bloco seguinte, ilustrado na Figura 7.


**Figura 7** Representação de uma lista de dados ligados [40]

As cadeias de blocos compreendem registos ou blocos de dados. À medida que cada transação ocorre, ela é colocada num bloco. Cada bloco é conectado ao bloco anterior e posterior, sendo adicionado ao próximo numa ordem irreversível e as transações são armazenadas juntas. Depois dos blocos serem guardados e validados para armazenamento no *ledger*, não podem ser alterados ou excluídos por um único ponto/nó da rede [4][75].

Este sistema funciona com base numa estrutura descentralizada, ou distribuída, onde cada ponto/nó possui uma cópia integral ou parcial de todo o *blockchain ledger*. Qualquer alteração ao *ledger* pressupõe uma aceitação coletiva, não havendo a possibilidade de alterar ou acrescentar novos blocos sem que todos os pontos/nós pertencentes à rede aprovem a transação [76][77].

A estrutura de um bloco de transações contempla dois componentes-chave [78]:

1. O cabeçalho do bloco – *Block header* – constituído pelo *hash value* do bloco anterior, informações relativas ao processo de *mining* necessário para validação do bloco e o código *Merkle Root* [52];
2. O identificador do bloco – *Block identifier* – composto pela assinatura digital correspondente ao bloco, gerada através de *hashing* com criptografia assimétrica.

A Figura 8 mostra a estrutura de um bloco de transações e os seus componentes.

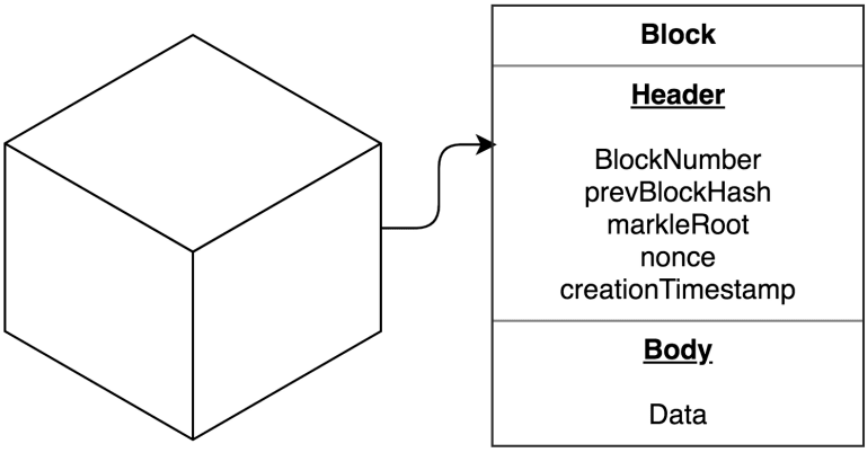


**Figura 8** Estrutura de um bloco de transações [79]

O *block number* é o número que representa a ordem de criação do bloco na rede. No fundo, é a posição do bloco na *blockchain*. O *previous block hash* refere-se ao *hash value* do bloco anterior. Conforme apresentado anteriormente, é esta ligação que garante a robustez e rastreabilidade da tecnologia. A *Merkle Root* contempla o código único que compreende todas as transações guardadas no bloco [74]. O "*nonce*" – *number only used once* – é um número de *32-bits* relacionado com o processo de *mining* [80]. O *nonce* representa a dificuldade do problema para o qual os pontos/nós da rede têm de encontrar a solução. O *timestamp* é data e hora de criação do bloco, que garante a singularidade do mesmo [79].

### 2.2.5. CONCEITO DE MINING

Conforme abordado nos pontos 2.3.3. e 2.3.4., a segurança e integridade da informação dos blocos pertencentes à *blockchain* é conseguida utilizando o *hash value* do bloco anterior para criar o seguinte [10][25][81]. A criação de um bloco envolve a validação por parte dos pontos/nós referentes à rede. Esta validação do *hash value* criado para o novo bloco tem o nome de *mining* [52]. Os pontos/nós responsáveis pela validação, são denominados de *miners* [52].

Este conceito agrega o processamento de *Merkle Trees* para chegar à *hash* da *Merkle Root*, código que representa a informação das transações presentes num bloco. Ao resultado, dá-se o nome de *Proof-Of-Work* (PoW) [82]. Uma *Proof-Of-Work* (PoW) pode ser definida

como um conjunto de operações matemáticas difíceis de resolver, mas cuja solução correta é fácil de verificar [6].

A Figura 9 demonstra o fluxograma das operações executadas por cada *miner* [52]. Essencialmente, o conceito de *mining* assenta numa competição entre os diferentes *miners* – pontos/nós da rede – para criarem novos blocos. Um *miner* está constantemente a atualizar a informação que possui da *blockchain*, guardando as novas transações numa *transaction pool* – *pool* de transações – e estando disponível para receber novos blocos (caso estes tenham sido verificados por outro miner). Este processo de atualização corre em *background*, isto é, havendo um novo problema para resolver – novo bloco para confirmar – o *miner* utiliza a capacidade de processamento para encontrar a solução, a PoW. Entretanto, qualquer transação nova que surja durante o processo de *mining*, é armazenada na *transaction pool* até poder ser integrada no novo bloco. Quando a solução é encontrada, a cópia da *blockchain* é atualizada recebendo o novo bloco e verificando o mesmo, e as transações presentes na *transaction pool* são eliminadas, dando espaço para novas transações e uma nova competição para a geração de um novo bloco [52][83].

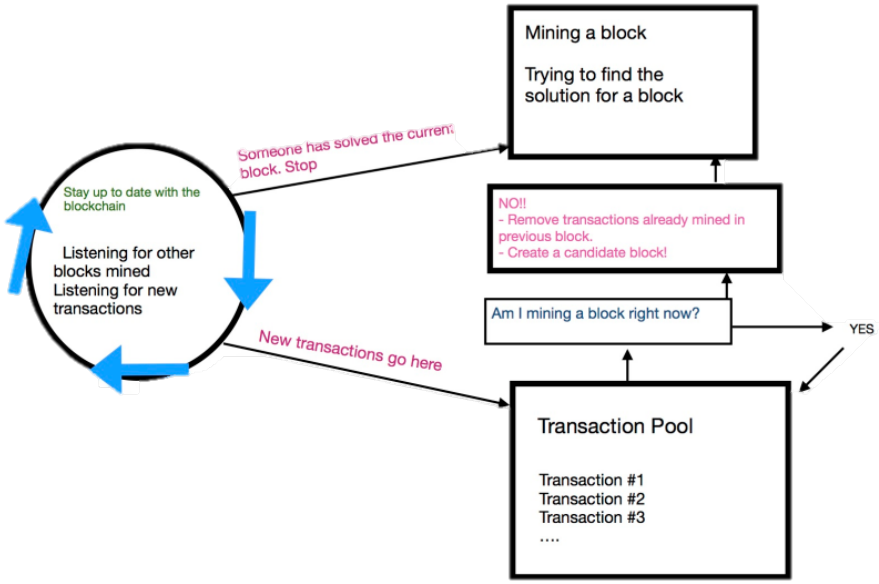


**Figura 9** Fluxograma do processo de um *miner* [52]

No momento em que a solução para o bloco é encontrada e este é enviado para todos os pontos/nós da rede, todos validam o bloco de acordo com as mesmas regras de forma a aceitarem o mesmo na *blockchain*. Esta validação apenas tem como objeto o bloco em si,

uma vez que a "corrida" para encontrar a PoW já terminou. Algumas das regras encontradas para blocos válidos nas aplicações de tecnologia *blockchain* são [52]:

- O *hash value* do *header* do bloco é menor do que o de destino;
- O tamanho do bloco está dentro dos limites aceitáveis;
- O registo de data e hora do bloco é inferior a um limite de tempo no futuro;
- A primeira transação, e apenas a primeira, é uma transação *coinbase* (aplicado no âmbito das criptomoedas);
- A transação *coinbase* tem uma recompensa válida (aplicado no âmbito das criptomoedas);
- Todas as transações dentro do bloco são válidas;

A transação *coinbase* é aplicada no domínio das criptomoedas. Esta transação contém a informação da recompensa para o *miner* que resolver a PoW [52][84]. A criação é feita no início de cada bloco e é criada por cada um dos pontos/nós da rede individualmente. O bloco que conseguir resolver a PoW ganha a recompensa por ele gerada. Os restantes blocos pertencentes aos outros pontos/nós da rede, são descartados [52].

A aplicação das regras de validação para novos blocos garante que toda a rede descentralizada aceita o bloco como válido, ou descarta o bloco como inválido. Se o bloco for válido, todos os pontos/nós da rede atualizam a sua cópia da *blockchain*. Isto garante um consenso distribuído – ou *distributed consensus* – entre todos os pontos/nós [25][36][52][66].

### 2.2.6. BLOCKCHAIN LEDGER

A tecnologia *blockchain* fornece um *ledger* imutável, distribuído por vários pontos/nós através de uma arquitetura descentralizada e tecnologias avançadas de computação [48]. Devido ao seu funcionamento e arquitetura, mantém um histórico inalterável, transparente e rastreável das atividades dos pontos/nós pertencentes à rede [76].

As características inerentes à arquitetura e estrutura da *blockchain*, garantem propriedades como a transparência, robustez e segurança [10][62]. Um *blockchain ledger* pode ser considerado uma base de dados distribuída que está organizada como uma lista

ordenada de blocos [42]. De certa forma, o *ledger* pode ser considerado uma estrutura distribuída de registos de data e hora.

A tecnologia *blockchain* permite uma rede P2P descentralizada onde os pontos/nós constituintes interagem de forma a que não haja uma autoridade central, um intermediário, para assegurar a confiança e legitimidade das transações [10]. Para alcançar esta forma de funcionamento, os autores *Fran Casino*, *Thomas K. Dasaklis* e *Constantinos Patsakis* apresentam um conjunto de mecanismos interconectados que fornecem as características específicas a esta infraestrutura [42]. A figura 10 mostra a arquitetura da *blockchain* desenhada pelos autores [42].

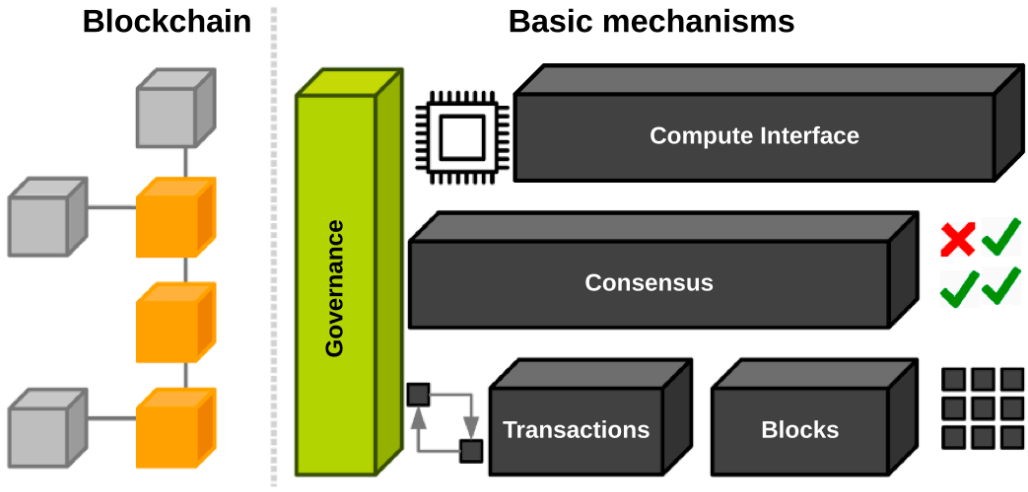


**Figura 10** Arquitetura de uma *blockchain* [42]

No nível mais baixo da infraestrutura, estão as transações (*Transactions*) entre os pontos/nós da rede, armazenadas em blocos (*Blocks*). Estas transações equivalem a um acordo entre, pelo menos, duas partes, podendo envolver a transferência de bens físicos ou digitais, a conclusão de uma tarefa, ou outra informação. Pelo menos uma das partes assina o bloco de transações, sendo o mesmo partilhado com os restantes pontos/nós para validação e verificação [42].

A validação e verificação dos blocos gerados é representada na segunda camada exibida na Figura 10 – *Consensus*. O mecanismo para atingir o consenso (*Consensus*) entre os diferentes pontos/nós varia de acordo com o tipo de *blockchain* [85]. Existem diversos

algoritmos para o chamado *distributed consensus*, sendo o mais conhecido o *Proof-of-Work* (PoW) [65][86]. No entanto, outros algoritmos como *Proof-of-Stake* (PoS) [87][88] ou *Byzantine Fault Tolerance* (BFT) [89][90] são igualmente utilizados para este efeito [42].

Uma camada adicional permite à *blockchain* oferecer mais funcionalidades. Esta camada – *Compute Interface* – permite o processamento de informação e cálculo de estados de diferentes pontos/nós pertencentes à rede. No caso das criptomoedas, por exemplo, a *blockchain* calcula o valor da carteira atual de cada ponto/nó, garantido uma atualização constante e transparente. Noutros casos mais complexos, a execução de transações automáticas, tendo como base determinadas condições específicas, pode ser garantida através do uso de *Smart Contracts* (SC) [42][43].

Por último, a camada relativa a *Governance* estende a arquitetura da *blockchain* de modo a incluir as interações humanas existentes no mundo físico. Apesar dos protocolos existentes na *blockchain* serem bem definidos, estes carecem, muitas vezes, de *inputs* manuais. Por esta razão, esta camada constitui a ponte entre os processos fora da *blockchain* e a própria *blockchain*, garantindo um conjunto de regras acerca da forma como os *inputs* devem ser considerados e utilizados [42].

Podemos distinguir dois tipos de *blockchain ledger* de acordo com o controlo de acessos – autenticação – e responsabilidade de validação de blocos – autorização [3][91][92][93]. *Permissionless ledgers*, são tipos de *blockchain* que residem no domínio público, por exemplo, a *Bitcoin* [8]. *Permissioned ledgers*, são tipos de *blockchain* governados por um conjunto de pontos/nós, ou seja, as validações de blocos e transações são feitas apenas por um conjunto de pontos/nós responsáveis pela criação dos mesmos. Este último tipo de *blockchain* reside fora do domínio público [18].

No entanto, a noção entre *blockchain ledgers* públicos ou *permissionless* e privados ou *permissioned* pode ser ambígua. A diferença assenta em dois conceitos-chave [25]:

- Autenticação – Indica quem pode aceder ao *blockchain ledger* (público ou privado);
- Autorização – Indica o que os participantes, pontos/nós, da rede podem fazer na *blockchain* (*permissioned* ou *permissionless*).

É possível a adoção de um tipo de *blockchain ledger* híbrido onde os diferentes modelos de autenticação e autorização podem ser conjugados e coexistir de acordo com regras inicialmente estabelecidas [48]. Uma observação feita pelos autores *Yingli Wang*, *Jeong Hugh* e *Paul Beynon-Davies*, mostra uma maior adoção de soluções do tipo *permissioned blockchain* [4]. Esta adoção poderá dever-se ao facto de *blockchain ledgers* do tipo *permissioned* serem mais eficazes no controlo da consistência e integridade da informação armazenada [4].

## 2.3. CONSENSUS NA BLOCKCHAIN

A tecnologia *blockchain* assegura a integridade do sistema descentralizado através de um algoritmo de consenso, ou *consensus* [66]. O uso de algoritmos deste género traduz-se no benefício da transparência do sistema em tempo real. Um algoritmo de *consensus* é o acordo entre os diferentes pontos/nós do *ledger* para a criação de blocos de transações na *blockchain* [10][94][95]. Em suma, um algoritmo de *consensus* pode ser definido como o mecanismo pelo qual a rede *blockchain* atinge o consenso na validação e verificação de transações [96]. Estes algoritmos asseguram que as regras do protocolo de comunicação são seguidas e garantem que todas as transações ocorrem de forma segura e confiável [66].

Um protocolo pode ser definido como um conjunto de regras base necessárias para o funcionamento da *blockchain*. Por sua vez, um algoritmo é definido como um mecanismo através do qual o protocolo será mantido, isto é, que assegura o cumprimento das regras base estabelecidas [96].

Existem diversos algoritmos de *consensus* dentro da tecnologia *blockchain*. A Figura 11 apresenta um infográfico ilustrativo da variedade de algoritmos existentes por tipologia de funcionamento [97].

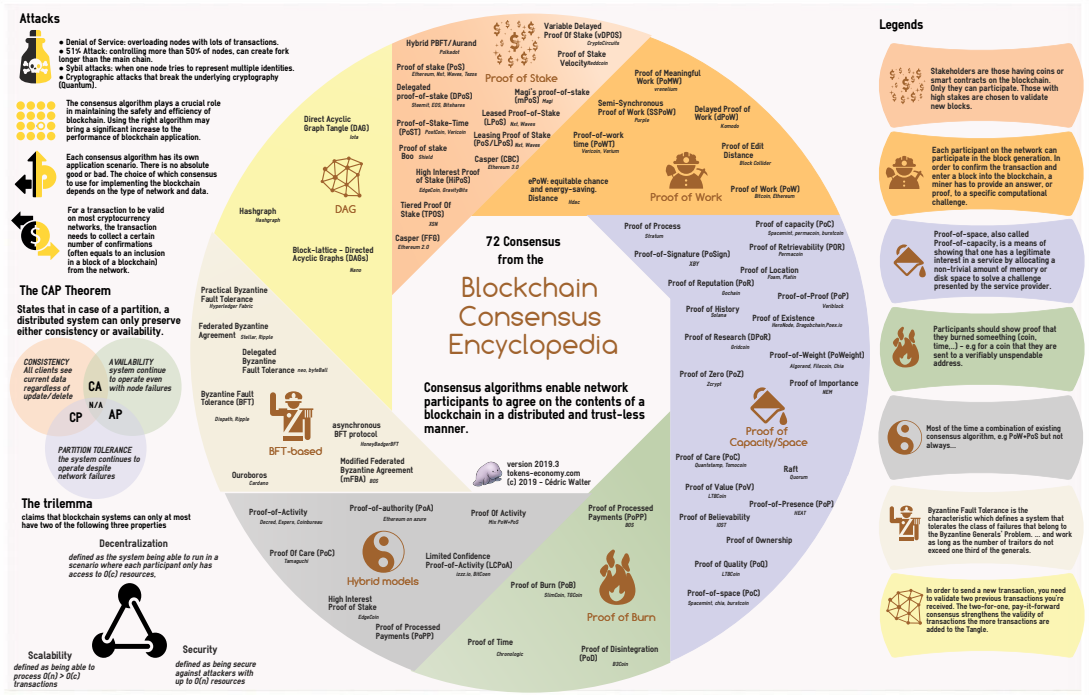


**Figura 11** Infográfico de algoritmos de *consensus* aplicados na *blockchain* [97]

Os algoritmos de *consensus* podem ser categorizados em oito domínios diferentes [98]:

1. Algoritmos baseados em *Proof-of-Work* (PoW);
2. Algoritmos baseados em *Proof-of-Stake* (PoS);
3. Algoritmos baseados em *Byzantine Fault Tolerance* (BFT);
4. Algoritmos híbridos baseados em *Proof-of-Activity* (PoA);
5. Algoritmos baseados em *Proof-of-Burn* (PoB);
6. Algoritmos baseados em *Proof-of-Capacity/Space* (PoC);
7. Algoritmos baseados em *Trusting Computing* (PoET);
8. Algoritmos baseados em *Direct Acyclic Graph* (DAG).

Cada algoritmo de *consensus* tem o seu próprio quadro de aplicação. A escolha do algoritmo de *consensus* a implementar na *blockchain* depende do tipo de rede e dados pretendidos [99].

### 2.3.1. PROOF-OF-WORK (POW)

O algoritmo PoW foi inicialmente desenvolvido com o intuito de combater o *email spamming*, originalmente apresentado em 2002 por Adam Back [100][101]. Em 2008, com a criação da *Bitcoin* [8], o algoritmo PoW foi introduzido e adaptado à realidade da

tecnologia *blockchain* para garantir o consenso e veracidade nas transações criadas na rede [101].

Este algoritmo de consenso agrupa as transações na forma de blocos. Os *miners* verificam a legitimidade das transações inseridas nos blocos, resolvendo um problema matemático – conhecido como *proof-of-work*. Após a resolução do problema, o *miner* que o resolveu primeiro é recompensado. Desta forma, as transações verificadas são guardadas na *blockchain* através de blocos [101].

Alguns aspetos negativos [101] do uso deste algoritmo assentam em:

- Fraca performance;
- PoW utiliza uma enorme quantidade de poder computacional, o que, por si só, reduz o incentivo de participação numa *blockchain* com este algoritmo;
- É vulnerável a ataques, uma vez que o potencial atacante conseguiria corromper a *blockchain* detendo 51% dos recursos de *mining* da rede (o que não é de todo fácil, embora possível);
- Ao longo do tempo as recompensas pelo *mining* de blocos vão reduzindo;
- Limita os inputs na estrutura de um algoritmo de *mining* numa *blockchain*,

No entanto, há igualmente aspetos positivos [101] a considerar:

- É o algoritmo mais antigo e seguro (é necessário um poder de processamento enorme para corromper uma *blockchain* com PoW);
- As taxas de transação não são obrigatórias;
- As soluções do problema matemático sugerido são facilmente verificáveis;
- As soluções do problema matemático sugerido são difíceis de resolver e passíveis de serem quantificáveis.

### 2.3.2. PROOF-OF-STAKE (POS)

O algoritmo PoW necessita de um grande poder de processamento computacional de forma a conseguir resolver os problemas criptográficos de forma a criar novos blocos – *mining* [102]. Esta capacidade traduz-se num alto nível de consumo elétrico de forma a

garantir a exequibilidade do algoritmo. Em 2015, foi estimado que uma transação na rede *Bitcoin* requeria eletricidade suficiente para alimentar 1,57 casas na América por dia [102].

O algoritmo PoS foi desenvolvido como uma alternativa à forma de consenso presente no algoritmo PoW [103][104]. Em alternativa ao conceito de *mining* no PoW, é aplicado o conceito de *stake coins* (moedas de jogo). Isto significa que a probabilidade de um nó criar o próximo bloco da *blockchain* é igual à percentagem de moedas na carteira em relação ao total da rede [104]. Ou seja, se um nó possui o equivalente a 5% do valor da rede, irá ter 5% de hipóteses de ser o criador do próximo bloco da *blockchain* e, por conseguinte, receber a recompensa (caso seja aplicável).

Apesar de o algoritmo conseguir ser corrompido mais facilmente do que no PoW, a consequência traduz-se na perda de todo o valor existente no nó que tentou corromper a *blockchain* [102]. Isto significa que, cada ataque à *blockchain* tem como consequência a perda total da stake existente no nó corrupto. Esta perda reflete-se numa probabilidade de 0% aquando a criação do bloco seguinte, "eliminando" o nó corrupto da lista de possíveis candidatos. Pode ser mais "fácil", mas as consequências são igualmente mais severas.

### 2.3.3. BYZANTINE FAULT TOLERANCE (BFT)

O algoritmo BFT remonta ao problema computacional clássico apresentado em 1982 [105]. O objetivo é garantir que um qualquer sistema computacional é capaz de continuar operacional mesmo que existam problemas funcionais ou informação conflituosa.

Este problema é ilustrado através de uma história. Existem diversos generais bizantinos com as suas respetivas tropas. Estes generais cercaram uma cidade inimiga, no entanto, estão fisicamente separados e isolados por montes e vales. A troca de mensagens é exclusivamente feita por estafetas mensageiros. O objetivo é conseguir conquistar a cidade inimiga. Para este feito, é necessário que todos os generais ataquem em uníssono ou retirem em uníssono. Caso contrário o ataque é malsucedido [102][105].

O problema surge na veracidade das mensagens enviadas pelos estafetas e pela resposta dos generais. Como podemos garantir que não existem traidores capazes de enviar mensagens conflituosas de modo a dispersar as tropas? Como garantimos o sucesso do ataque caso um estafeta seja apanhado pelo caminho ou morra?

Numa *blockchain*, este enunciado traduz-se na necessidade que os diferentes nós da rede (generais) têm para garantir o consenso (ataque sincronizado) de modo a poderem criar novos blocos e aceitar novas transações. As dificuldades prendem-se na possibilidade de uma mensagem ser perdida (estafeta falhar) ou haver nós corruptos (mensagens conflituosas do general corrupto) e, ainda assim, a rede conseguir certificar a veracidade das transações/blocos de forma transparente.

Em 1999 foi apresentada uma das primeiras soluções para este problema, intitulada como *Practical Byzantine Fault Tolerance*, ou PBFT [106]. Hoje, esta solução é utilizada em alguns *distributed ledgers*, incluindo o *Hyperledger Fabric* [107]. Neste último caso, apresenta até 20 "generais" pré-selecionados de forma a garantir o consenso eficiente da rede, garantindo maior fluxo de transações.

Outras soluções têm vindo a ser estudadas e aplicadas no âmbito da *blockchain*. O caso de *Federated Byzantine Agreement* (FBA) [108], utilizada em redes como a *Stellar*, *Ripple* ou *Dispatch*. De igual forma, a solução *Delegated Byzantine Fault Tolerance* (DBFT), utilizada maioritariamente pela rede *Neo* [109].

Esta forma de gerar consenso em *distributed ledgers* permite um maior fluxo de transações e uma rápida escalabilidade de soluções. No entanto, é maioritariamente utilizada em *blockchains* do tipo *permissioned* ou privadas.

### 2.3.4. PROOF-OF-ACTIVITY (POA)

A forma de consenso do algoritmo PoA combina componentes de PoW com PoS [110][111]. O *mining* inicia de forma tradicional, através da resolução de um problema computacional. A diferença encontra-se nos blocos que os *miners* geram não conterem transações. Estes blocos são apenas modelos com informações de cabeçalho (*header*) e o endereço que irá receber a recompensa [111].

No momento em que o bloco é criado e o conteúdo acedido pelo *miner* que resolveu o problema, o sistema muda o protocolo de consenso para PoS. Neste ponto, as informações do cabeçalho (*header*) são utilizadas para selecionar um grupo de *validators* para assinar o bloco de transações. Um destes *validators* pré-definidos no *header* do bloco modelo

minerado, será escolhido tendo em conta a *stake* que possui (funcionando da mesma forma que o PoS) [110][111].

### 2.3.5. PROOF-OF-BURN (POB)

O algoritmo PoB assenta no conceito de "queimar" moedas (*stake coins*) em troca de aumentar a probabilidade de criar o bloco seguinte [112][113][114]. Ao invés de tentar resolver um problema computacional, os nós da rede enviam *stake coin*s para um endereço onde são irrecuperáveis [113]. A premissa de consenso baseia-se na assunção de que ao queimar *stake coins*, o nó da rede garante estar a seguir o protocolo de consenso, uma vez que está a abdicar de forma autónoma de parte da sua *stake* [112]. Com isto, é garantido um privilégio vitalício para o *mining* da rede baseado num processo de seleção aleatório [114].

Este algoritmo aumenta a segurança da rede de acordo com o volume de transações da mesma, uma vez que, ao existir *stakes* maiores, será necessário "queimar" mais para poder garantir o consenso. Este funcionamento torna demasiado dispendioso o ataque à *blockchain* [114].

Outro ponto favorável é a não compensação por *stakes* grandes. No PoS, quanto maior a *stake* do nó, maior a probabilidade de este ser o criador do próximo bloco. No PoB, esta premissa não se aplica. Ao "queimar" *stake coins*, o nó entra num processo de seleção completamente aleatório para poder ser o criador do bloco seguinte e, por conseguinte, receber a recompensa. Desta forma, *stakes* grandes não obtêm vantagem sobre outras *stakes* mais pequenas [113]. No entanto, conforme referido anteriormente, a "queima" de *stake* coins não garante a concretização do bloco seguinte [114].

### 2.3.6. PROOF-OF-CAPACITY/SPACE (POC)

Praticamente todos os algoritmos são, numa primeira instância, comparáveis ao PoW no sentido em que tentam resolver o problema de consumo excessivo de capacidade computacional para atingir consenso na *blockchain* [101]. O PoC assume um funcionamento diferente que permite a utilização do espaço em disco e do uso do disco rígido para efeitos de *mining* [115].

O processo pode ser visto como um PoW condensado, onde os *miners* apenas computam a *blockchain* uma vez (num processo chamado *plotting*) e guardam os resultados em cache no disco rígido [115]. O conceito de *mining* surge de forma diferente, apenas sendo necessário ler a informação armazenada em cache, assegurando um tempo reduzido por bloco armazenado [115].

O termo *plotting* é o nome para o espaço de armazenamento dedicado ao uso para cálculos na rede *Burstcoin* [116]. Um *plot* é um arquivo que contém *hashes* pré-calculadas que podem ser usadas para gerar novos blocos para a *blockchain Burstcoin* [116]. Este algoritmo e algumas variantes do mesmo, são utilizados em redes como *SpaceMint* [117] e *Permacoin* [118].

### 2.3.7. PROOF-OF-ELAPSED-TIME (POET)

Este tipo de algoritmo de consenso é, maioritariamente, utilizado em *blockchains* do tipo *permissioned* [119]. Isto é, redes onde é necessário que os potenciais participantes da rede se identifiquem e façam prova da sua identidade antes de acederem à rede.

O algoritmo PoET é usado para decidir quem terá os direitos de criar o bloco seguinte da rede (*mining*). Esta decisão é baseada no princípio de um sistema justo de lotaria, onde todos os nós/participantes da rede têm a mesma hipótese de ganhar [119][120].

O mecanismo PoET, utilizado, por exemplo, no *Hyperledger Sawtooth* [121], atribui aos participantes da rede um tempo de espera aleatório. O primeiro participante a terminar o tempo de espera atribuído será o vencedor e, como tal, o responsável por criar o bloco seguinte da rede [120].

### 2.3.8. DIRECT ACYCLIC GRAPH TANGLE (DAG)

Este mecanismo de consenso implica a validação dos dois blocos anteriores de forma a criar o bloco seguinte. Funciona com base no modelo de grafos acíclicos dirigidos, onde para a criação de um novo bloco “n” é necessário que os blocos “n-1” e “n-2” sejam verificados e validados [122]. A Figura 12 representa as interações individuais entre blocos de acordo com este funcionamento [123].

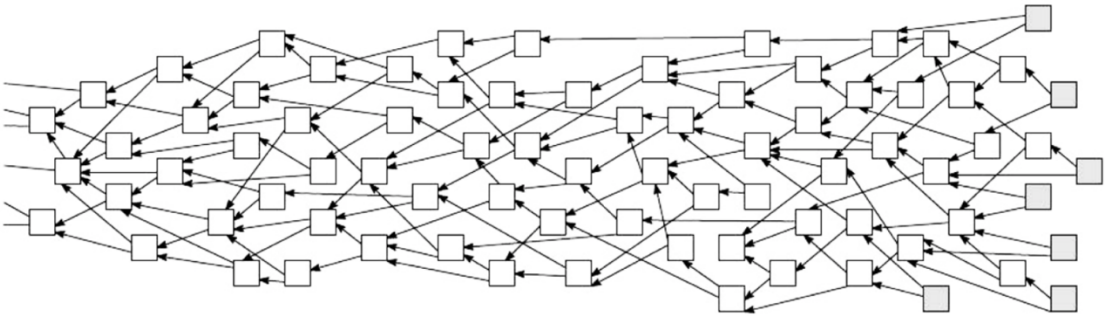

**Figura 12** - Interações entre blocos no mecanismo DAG (*Tangle*) [123]

Este algoritmo de consenso é utilizado na rede *Iota* [124]. O funcionamento traduz-se numa maior eficiência de consumo energético uma vez que as transações são, em geral, mais pequenas [123][125]. É escalável, garantindo mais segurança quanto maior for o número de transações [123]. No entanto, caso um nó seja responsável pela criação de mais de um terço dos blocos (>33%), poderá corromper a rede [125]. Para evitar este ataque à rede, a *Iota* possui um nó que verifica todas as transações em paralelo com o funcionamento normal. Este nó, chamado de "*The Coordinator*" (Coordenador) é responsável por uma segunda verificação à rede, de forma a evitar ataques e blocos corrompidos [123][124]. Assim que a rede atinga um volume de blocos grande o suficiente para não ser possível ataques superiores a 33%, o bloco Coordenador será desativado. Outro ponto menos positivo é a não existência de lógica para *smart contracts* [123].

# 3. DOMÍNIOS DE APLICAÇÃO DA BLOCKCHAIN

A tecnologia *blockchain* apresenta novas características para o mundo empresarial e industrial [126]. Esta tecnologia permite o armazenamento seguro de informação de uma forma descentralizada, incorporando vários mecanismos que garantem a imutabilidade, rastreabilidade e transparência da informação. A estrutura associada à *blockchain* não depende de nenhuma autoridade central ou intermediário para assegurar a confiança da rede, mostrando-se como uma solução face às limitações de estruturas centralizadas [76].

Apesar da tecnologia *blockchain* estar numa fase inicial de comercialização e aplicação, há uma enorme especulação em relação ao futuro desta tecnologia [61]. As potenciais aplicações em diversas áreas para além das criptomoedas e a versatilidade dos desenvolvimentos conseguidos nos últimos anos, aumentam a expectativa em relação à *blockchain*, havendo atualmente várias aplicações implementadas em diversas indústrias [48].

A título de exemplo, a *Everledger* [127][128] é uma empresa que desenvolveu um *blockchain ledger* para a certificação de diamantes. De modo a combater a contrafação e os "diamantes de sangue", foram desenvolvidos certificados digitais atribuídos a cada diamante através de uma *blockchain* partilhada mundialmente [57].

A *Hyperledger* [129] é uma comunidade colaborativa que engloba diferentes indústrias. Tem como objetivo desenvolver um conjunto de *frameworks*, ferramentas e bibliotecas de programação que apoiem na implementação de tecnologia *blockchain* [130][131].

Outro exemplo do desenvolvimento tecnológico presente nesta tecnologia disruptiva é evidente na plataforma *Ethereum* [132]. A *Ethereum*, para além de servir como base à própria criptomoeda, oferece máquinas virtuais (*virtual machines* – VM) descentralizadas para a execução de *Smart Contracts* (SC) [133][134].

Este capítulo apresenta os *Smart Contracts* na tecnologia *blockchain*, tentando dar uma explicação acerca do seu funcionamento, utilização e exemplos de aplicação. Este capítulo pretende, de igual forma, abordar os diferentes domínios de aplicação da tecnologia *blockchain* para além das criptomoedas, dando exemplos encontrados na literatura científica.

## 3.1. SMART CONTRACTS

Baseado no princípio da descentralização apresentado pela tecnologia *blockchain*, onde autoridades centrais ou intermediários são eliminados, o *Smart Contract* torna-se uma aplicação essencial da *blockchain* [13]. Este desenvolvimento contribui para a redução de custos, aumento de rastreabilidade, visibilidade e segurança da informação na rede [10][135][136]. As aplicações deste mecanismo automático são diversas, alavancando as vantagens trazidas pela *blockchain* em relação à transparência, confiança e eficiência na comunicação entre diferentes partes [9][76][137].

A definição de *Smart Contract* foi apresentada pelo autor *Nick Szabo* como "*a computerised transaction protocol that executes the terms of a contract*" [106][107]. Isto é, uma transação protocolar computorizada que executa os termos de um contrato estabelecido. Este mecanismo permite traduzir cláusulas contratuais para código de programação, dentro de uma *blockchain*. Desta forma é possível reduzir o número de intervenientes participantes na execução de um contrato, mitigando os riscos adjacentes [42].

Em suma, um *Smart Contract* é um acordo entre diferentes partes que, apesar de não se conhecerem dentro da *blockchain*, conseguem acordar termos que são automaticamente satisfeitos em conformidade com as condições estabelecidas. Desta forma, os *Smart Contracts* são executados de uma forma descentralizada e guardados na *blockchain* sem necessitarem de uma autoridade central ou intermediário que ateste a veracidade do mesmo [10][140]. A Figura 13 exemplifica o funcionamento de um *Smart Contract* [141].

Numa *blockchain*, um *Smart Contract* é criado entre duas entidades/nós da rede. Estas entidades permanecem anónimas perante a restante rede e o contrato estabelecido é armazenado num *ledger*. Quando as condições pré-estabelecidas do *Smart Contract* são atingidas (tempo, ações ou eventos), este é executado de forma autónoma entre as

entidades acordadas. Esta forma de atuação permite que todos os contratos efetuados numa *blockchain* possam ser analisados e auditados [141].

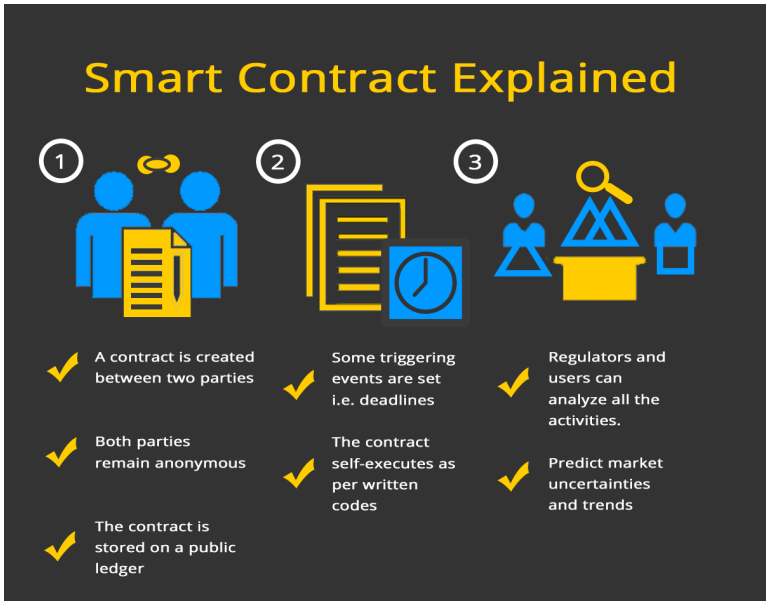


**Figura 13** Explicação sobre o funcionamento de um *Smart Contract* [141]

Um *Smart Contract* pode ser parcial ou totalmente executado, podendo ser monitorizado por todos os pontos/nós da rede [142]. Este mecanismo torna possível transações automáticas e a troca de ativos digitais ou físicos na forma de *tokens* implementados através de *Smart Contracts* na *blockchain* [138][139][143].

Um exemplo comum da aplicabilidade dos *Smart Contracts*, pode ser dado através da compra e venda de um imóvel [141]. O processo tradicional implica uma quantidade de intermediários até que seja possível obter autorização para efetuar a compra. Após a autorização, são igualmente requeridos mediadores para atestar a troca de propriedade e concluir a compra e venda do imóvel. Com a utilização de *Smart Contracts*, é possível eliminar todos os intermediários e, com isso, reduzir o tempo e custos do processo. Isto acontece, porque a *blockchain* certifica a veracidade da informação entre as partes e a identidade das mesmas. Devido à característica imutável da rede, é possível auditar e monitorizar a troca de propriedade entre as diferentes partes.

Alguns domínios de aplicação deste mecanismo automático podem ser vistos na Figura 14 [141]. Armazenamento de registos, atividades comerciais, cadeia de abastecimento,

sistema de hipotecas, mercado imobiliário, contratos empresariais, proteção de direitos de autor, serviços de saúde, sistemas de eleições, reivindicações de seguro e *Internet-of-Things*, são alguns dos domínios identificados que beneficiam com a aplicação de *Smart Contracts*.


**Figura 14** Domínios de aplicação de *Smart Contracts* [141]

Alguns exemplos da forma como podem ser aplicados nos diversos domínios são [10][141]:

- Os *Smart Contracts* podem armazenar registos, transacioná-los e atualizá-los automaticamente sempre que for necessário. Mais ainda, caso haja necessidade ou exigência de remover qualquer registo de forma permanentemente por lei (por exemplo, Regulamento Geral sobre a Proteção de Dados), o funcionamento da tecnologia permite que isto seja feito de forma automática;
- No âmbito de atividades comerciais, bancárias ou não, é possível eliminar o intermediário da transação, evitando assim custos e entropia no que diz respeito ao tempo de execução da transação;
- Na área da cadeia de abastecimento logística, é possível garantir, através de *Smart Contracts*, um registo transparente do estado, localização e origem dos materiais transacionados. Esta rastreabilidade verificada (através da *blockchain*) possui um potencial de impacto nesta área;

- No sistema de hipotecas, ou financiamento imobiliário, são exigidos documentos que comprovem rendimentos, identidade, despesas, créditos, e outras informações do lado do proprietário e do hipotecário. Com a tecnologia *blockchain* e utilização de *Smart Contracts*, é possível obter e validar estas informações de forma instantânea, desde que haja o consentimento de ambas as partes para tal transação (neste caso, de informação);
- No mercado imobiliário, anteriormente exemplificado, podemos assistir a uma forma de redução de custos e do tempo do processo de compra e venda de imóveis;
- No seio empresarial, todos os dias são celebrados contratos. Sejam de trabalho para os colaboradores, sejam entre fornecedores ou clientes, existe um ponto comum, o tempo e a burocracia necessários para celebrar os termos dos contratos. Com recurso à *blockchain* em conjunto com *Smart Contracts* bem estabelecidos, é possível garantir um processo mais transparente e célere;
- Os direitos de propriedade intelectual são um domínio importante para o uso de *blockchain* e *Smart Contracts*. Esta tecnologia permite a validade do autor e ao mesmo tempo a garantia de que não poderá existir uma cópia contrafeita sobre a propriedade intelectual do mesmo, devido à sua característica imutável e auditável;
- Nos serviços de saúde, os registos e histórico dos pacientes encontra-se, por vezes, centralizado entre grupos de hospitais ou confinados ao espaço territorial. Com uma ampla adoção da tecnologia neste setor, poderia ser possível que os registos clínicos e histórico médico de um paciente fossem acessíveis em qualquer lado, desde que houvesse o consentimento para consulta do próprio paciente;
- Os sistemas de eleições, ou votos, começam a iniciar um caminho para garantir o voto digital. No entanto, existe a possibilidade de corrupção e fraude em sistemas de voto digital centralizados. O recurso a *Smart Contracts* pode facilitar na validação de identidade e associação do voto ao eleitor, garantindo que não existem votos duplicados e/ou desvios dos mesmos;
- Nas seguradoras, a gestão de reclamações e coberturas pode acarretar um processo de comprovação do lesado longo e custoso. O recurso a uma rede *blockchain* com *Smart Contracts* pode automatizar o tratamento de algumas reclamações e, desta forma, acelerar o processo de reembolso ou tomada de decisão;

- No âmbito da *Internet-of-Things*, conforme abordado anteriormente, é possível imaginar um imenso potencial quando a tecnologia *blockchain* for conectada a diferentes máquinas, sensores ou outros dispositivos inteligentes.

Os *Smart Contracts* acarretam significativas implicações tecnológicas, legais e sociais. Isto deve-se ao facto de o funcionamento deste mecanismo poder alterar fundamentalmente as estruturas organizacionais e respetivas cadeias de abastecimento [144][145]. Estas barreiras podem demorar algum tempo a ser ultrapassadas, mas existem hoje diversas aplicações da tecnologia *blockchain* em áreas para além das criptomoedas [4].

## 3.2. BLOCKCHAIN PARA ALÉM DAS CRIPTOMOEDAS

Ao longo do tempo têm sido identificados diferentes domínios de aplicação da tecnologia *blokchain* que vão para além das criptomoedas e setor financeiro [9]. Alguns exemplos contemplam [18][48]:

- A *Walmart* testou uma aplicação que rastreia carne de porco na China para produção nos EUA, de modo a autenticar transações e aumentar a precisão e eficiência da manutenção dos registos;
- A *Maersk* e IBM estão a trabalhar juntas em transações entre fronteiras e entre partes que usam a tecnologia *blockchain* para ajudar a melhorar a eficiência do processo logístico de transporte;
- A BHP está a introduzir uma solução *blockchain* que substitui as folhas de registo físicas para rastrear amostras interna e externamente de vários fornecedores;
- A empresa *Provenance*, uma *start-up* do Reino Unido, arrecadou US$ 800.000 para adaptar a tecnologia *blockchain* para rastrear alimentos;
- Os autores Düdder e Ross apresentaram uma solução *blockchain* para o problema do rastreamento de madeira [146];
- O Grupo Renault está a desenvolver um protótipo de um sistema baseado em *blockchain* para armazenar as informações digitais dos seus veículos, de modo a fornecer uma única fonte de verdade para os dados de manutenção de cada automóvel;

- A *Bosch*, em parceria com uma autoridade de certificação alemã do setor automóvel, está a implementar um sistema baseado em *blockchain* para informações digitais de veículos, de modo a combater a manipulação ilegal de odómetros.

Estudos sobre a implementação da tecnologia *blockchain* constatam que as empresas que introduzem efetivamente a tecnologia *blockchain* têm maior probabilidade de obter ganhos maiores do que aquelas que não o fazem, principalmente por causa dos seus benefícios em termos de transparência da informação e redução de custos associados ao corte de intermediários [41][46][87][147][148][149].

### 3.2.1. SETOR DE ENERGIA ELÉTRICA

Um dos setores onde a tecnologia tem sido notória é o setor de energia elétrica [136][150][151][152][153][154][155]. Tendo por base o modelo tradicional de *bitcoin*, as redes inteligentes oferecem um mercado descentralizado no qual os consumidores (produtores e consumidores de energia ao mesmo tempo) podem negociar com outros consumidores sem qualquer parte intermediária ou autoridade central [9].

Cerca de 25% dos artigos científicos sobre aplicação de *blockchain* são relativos ao setor de energia elétrica [9]. Juntando os resultados atingidos nesta área, é possível afirmar que o setor de energia é visto como *benchmark* na implementação e casos de estudo da tecnologia *blockchain* e *Smart Contracts* [9].

### 3.2.2. APLICAÇÕES FINANCEIRAS

A tecnologia *blockchain* é aplicada a uma ampla variedade de campos financeiros, incluindo serviços de negócios, liquidação de ativos financeiros, mercados de previsão e transações económicas [156]. O sistema financeiro global tem explorado formas de usar aplicações *blockchain* para ativos financeiros [92].

Nesta área, podemos assistir a parcerias conjuntas entre bancos internacionalmente conhecidos para alavancar o potencial da *blockchain* [42]:

- O *Barclays* e a *Goldman Sachs* desenvolveram uma parceria com a R3 [157][158] para estabelecer uma estrutura operacional baseada em tecnologia *blockchain* para o mercado financeiro [156];
- A criação do primeiro grupo interbancário para pagamentos globais, tendo como base tecnologia *blockchain*. Deste grupo, fazem parte o *Bank of America Merrill Lynch*, *Santander*, *UniCredit*, *Standard Chartered*, *Westpac Banking Corporation*, e *Royal Bank of Canada*. A tecnologia *blockchain* tem como base a rede *Ripple* [159].

### 3.2.3. VERIFICAÇÃO DE INTEGRIDADE

As aplicações de verificação de integridade da tecnologia *blockchain* armazenam informações e transações relacionadas com a criação e o tempo de vida de produtos ou serviços. Algumas aplicações possíveis são [42]:

- Rastreabilidade de forma a garantir a validade da proveniência e evitar a falsificação de bens;
- Validação de identidade para efeitos de cobertura de seguros;
- Gestão de propriedade intelectual (IP).

O último ponto não está limitado apenas a arte ou cultura. Engloba o seu conceito mais amplo, como patentes, informação confidencial corporativa ou outro tipo de propriedade intelectual existente. O uso da tecnologia *blockchain*, garante, pela sua definição, a validade da integridade dos dados e transações presentes na rede.

### 3.2.4. GOVERNO E ESTADO

Ao longo dos anos, os governos são responsáveis por gerir e manter registos oficiais de cidadãos e empresas. Aplicações com uso de *blockchain* podem mudar a maneira como os governos operam ao nível local ou global, diminuindo intermediários das transações e manutenção de registos [160][161].

No uso consciente da identidade, é possível colocar do lado do utilizador o controlo no que diz respeito ao acesso e partilha de informações pessoais. Os dados ficam mais seguros, e é garantida a veracidade do sistema [161].

### 3.2.5. SERVIÇOS DE SAÚDE

A tecnologia *blockchain* pode desempenhar um papel central no setor da saúde, com várias aplicações em áreas como, gestão pública de assistência médica, registos de assistência médica, adjudicação automatizada de receitas, acesso *online* a pacientes, distribuição de dados médicos, pesquisa médica orientada ao utilizador, prevenir a falsificação de medicamentos, registos de ensaios clínicos e apoio na medicina de precisão [162][163][164][165].

### 3.2.6. PRIVACIDADE E SEGURANÇA

A *blockchain* é considerada uma oportunidade para melhorar os aspetos de segurança do fenómeno *big data* e ajudar na escalabilidade quando combinada com outros sistemas de armazenamento eficientes [166][167][168][169].

A *tecnololgia* pode ajudar a alcançar uma plataforma descentralizada baseada em *blockchain* P2P que compreende três tipos de entidades:

- Usuários, que interagem com as aplicações;
- Serviços, que fornecem tais aplicativos e processam os dados pessoais dos usuários por motivos operacionais e comerciais; e
- Nós, entidades que recebem recompensas em troca da manutenção do *blockchain*. Uma vez que apenas ponteiros de *hash* são armazenados, os usuários têm controle sobre seus dados.

### 3.2.7. APLICAÇÕES COMERCIAIS E INDUSTRIAIS

A *blockchain* tem o potencial de se tornar uma fonte significativa de inovações disruptivas nos negócios e na gestão, melhorando, otimizando e automatizando processos de negócios [170][171][172].

As aplicações baseadas em *blockchain* podem servir como sistemas de gestão descentralizados para várias empresas. Cada instância pode ser mantida na *blockchain* e o fluxo de informação executado através de *Smart Contracts*. Desta forma, os processos intraorganizacionais tornam-se mais ágeis e automáticos, traduzindo uma redução de custos para as empresas [42].

### 3.2.8. EDUCAÇÃO

A *blockchain* pode resolver problemas de vulnerabilidade, segurança e privacidade no caso de ambientes de aprendizagem ubíquos e pode ser usada para armazenar registos educacionais relacionados a recompensas de reputação [173][174][175].

O registo de resultados académicos e de créditos institucionais no âmbito de *European Credit Transfer and Accumulation System* – ECTS – são alguns exemplos práticos do uso das características relativas à *blockchain* [176]. Falamos da imutabilidade, veracidade da informação e prova de identidade dos participantes da rede. Desta forma, é possível que os registos académicos sejam validados de forma automática, reduzindo tempo e custo em tarefas burocráticas e administrativas, através da execução de *Smart Contracts* entre as instituições de ensino e os respetivos alunos.

### 3.2.9. GESTÃO DA CADEIA DE ABASTECIMENTO

É expectável que a tecnologia *blockchain* aumente a transparência e a confiança nas redes da cadeia de abastecimento, possibilitando cadeias de valor mais flexíveis [164][177][178][179]. As aplicações baseadas em *blockchain* na cadeia de abastecimento têm o potencial de gerar avanços em três áreas específicas [180]:

(i) Visibilidade;
(ii) Otimização;
(iii) Procura.

A tecnologia *blockchain* pode ser usada na área logística, ajudando na identificação de produtos contrafeitos, diminuindo o processamento da carga e utilização de papel, facilitando a rastreabilidade da origem e permitindo que compradores e vendedores negociem diretamente, sem a manipulação de intermediários [47].

Foi demonstrado que o uso de aplicações baseadas em *blockchain* em redes de *supply chain* pode aumentar a segurança [181], levar a mecanismos de gestão de contratos mais robustos entre a logística de terceiros e para terceiros [182], combater a assimetria de informação e melhorar os mecanismos de rastreamento e garantia de rastreabilidade [183], fornecer melhor gestão de informações para toda a cadeia de abastecimento [184],

melhorar a gestão de *stock* e desempenho em cadeias de abastecimento complexas [185] e, por fim, pode melhorar os sistemas de transporte inteligentes e oferecer novas arquiteturas de manufatura descentralizadas [186].

As diferentes áreas apresentadas neste capítulo servem para demonstrar a abrangência da tecnologia *blockchain*. Apesar desta tecnologia ter surgido no âmbito das criptomoedas, é notória a aplicabilidade noutras áreas [62], sendo o foco desta dissertação abordar a ligação à cadeia de abastecimento logística, os seus benefícios e dificuldades na sua implementação.

# 4. BLOCKCHAIN NA CADEIA DE ABASTECIMENTO (SUPPLY CHAIN)

Estudos recentes mostram uma forte inclinação para a adoção da tecnologia *blockchain* nas áreas de logística e cadeia de abastecimento [61][187]. Aplicações baseadas em *blockchain* têm o potencial para melhorar diversas áreas relativas à cadeia de abastecimento [42]. O recurso a esta tecnologia na logística pode apoiar na identificação de peças contrafeitas, diminuir o uso de papel físico, facilitar o rastreamento de material e permitir que compradores e vendedores possam interagir diretamente entre si sem recurso a entidades intermediárias [188][189][190][191][192][193].

Tem sido demonstrado que aplicações baseadas em *blockchain* aumentam a segurança da rede logística, tornam mais robustos os mecanismos de gestão de contratos entre diferentes partes, combatem informação redundante ou réplicas desatualizadas, e garantem mecanismos de rastreamento mais robustos através de informação fiável e imutável [42].

Este capítulo tem como objetivo abordar as especificidades da aplicação de tecnologia *blockchain* à cadeia de abastecimento. Inicia com um contexto sobre a definição de cadeia de abastecimento, tenta explicar a relação entre a tecnologia e a área de enfoque, seguem-se instruções sobre a implementação da tecnologia, culminando com uma apresentação sucinta dos *ledgers*, *Hyperledger Fabric*, *Hyperledger Sawtooth* e *Ethereum*. Neste capítulo são igualmente apresentados os benefícios e as limitações da tecnologia na área da cadeia de abastecimento – *supply chain* – e logística.

## 4.1. CADEIA DE ABASTECIMENTO (SUPPLY CHAIN)

A cadeia de abastecimento consiste na rede de organizações que estão envolvidas, através de ligações e interações, nos diferentes processos e atividades que produzem valor sobre a forma de produtos e serviços nas mãos do cliente final [6].

As cadeias de abastecimento estão cada vez mais complexas, difíceis em termos de tarefas e diversificadas em termos de partes interessadas. Muitas organizações não têm uma visão integrada de toda a cadeia de abastecimento. Grandes organizações construíram as suas próprias identidades e sistemas para manter uma cobertura global de operações e têm o poder de instruir os seus fornecedores. Caso contrário, é necessário o recurso a órgãos reguladores centralizados ou intermediários. Esta baixa transparência causa problemas e dificuldades no mecanismo da cadeia de abastecimento em termos de segurança, rastreabilidade, autenticação e sistema de verificação [48].

O fenómeno da gestão de cadeia de abastecimento surge na década de 1990, quando as empresas perceberam que as declarações normativas sobre a cadeia de abastecimento escritas na década de 1950 [194] precisavam de ser adaptadas na era de uma crescente competição global. Este conceito, gestão da cadeia de abastecimento, está mais uma vez em detalhado estudo e análise na era da indústria 4.0 com o rápido desenvolvimento de tecnologias baseadas em informação [195].

Podemos identificar quatro grandes mudanças de paradigma no âmbito das cadeias de abastecimento [195]. Em primeiro lugar, a mudança das preferências do cliente final na direção a ofertas cada vez mais exclusivas, juntamente com a inovação tecnológica, exigiram que as empresas encontrassem novas maneiras de acomodar essas necessidades de personalização. Em segundo lugar, os clientes passaram a procurar satisfação e excelência em todas as experiências de compra ou "jornada do cliente" que envolvem as etapas pelas quais eles passam no envolvimento com a empresa em termos de produto, serviço, compra, serviço pós-venda ou qualquer combinação [196]. Terceiro, os clientes estão a começar a pedir emprestado e experimentar os produtos, antes de os adquirir, pois percebem a satisfação não por meio da compra de produtos, mas por experimentá-los. Por fim, os clientes também se preocupam, cada vez mais, com os impactos de todas as suas

experiências de consumo no bem-estar económico, bem-estar pessoal e, mais recentemente, no bem-estar da sociedade e do meio ambiente [195].

Durante o ciclo de vida de um produto, à medida que ele atravessa a cadeia de valor (desde a produção ao consumo), os dados gerados em cada etapa podem ser documentados como uma transação, criando assim um histórico permanente do produto. A tecnologia *blockchain* pode contribuir efetivamente para:

(i) Registar cada ativo (do produto aos *containers*) à medida que flui através dos nós da cadeia de abastecimento;

(ii) Rastrear pedidos, recibos, faturas, pagamentos e qualquer outro documento oficial;

(iii) Rastrear ativos digitais (como garantias, certificações, direitos de autor, licenças, números de série, códigos de barras) de forma unificada e em paralelo com ativos físicos e outros [6].

Esta quantidade de interações e de informação entre cada nó da rede, enaltece a importância de uma cadeia de abastecimento transparente, traduzindo diversos desafios inerentes à área [25]:

- Gestão logística ineficiente;
- Falta de visibilidade de ativos;
- Tratamento impróprio de dados;
- Manuseio ineficiente da informação;
- Gestão de risco ineficaz.

As empresas procuram aplicar a tecnologia *blockchain* para aprimorar os sistemas de gestão e segurança. Com esta tecnologia, é possível reduzir custos, uma vez que a transparência inerente à tecnologia elimina a necessidade de vigilância e acompanhamento permanente de forma manual sobre as transações na cadeia de abastecimento [25].

O funcionamento da tecnologia aplicada na cadeia de abastecimento pode ser explicado da seguinte forma, quando a propriedade de um produto é transferida de uma parte para outra, o novo proprietário torna-se a única parte capaz de atualizar o estado do produto. Quando o novo proprietário processa ainda mais o produto e atualizar o estado do mesmo, estas novas informações são carregadas num bloco e armazenadas no *ledger* (*blockchain*). No entanto, para que as informações sejam armazenadas de forma definitiva na *blockchain*, o destinatário seguinte tem de concordar com as informações em questão. Caso o destinatário seguinte aceite o estado do produto, este é armazenado definitivamente na *blockchain* sendo compartilhada com todos os nós da rede [25].

A confiança é o fator mais influente que direciona o interesse na tecnologia *blockchain* dentro da gestão da cadeia de abastecimento. A confiança refere-se à confiabilidade das informações fornecidas pelos parceiros comerciais ou à segurança e proteção dos dados geridos por uma autoridade central [4].

As principais características da *blockchain* podem ser muito úteis para aplicar na cadeia de abastecimento. A disponibilidade pública permite rastrear produtos desde o local de origem até ao cliente final. A estrutura descentralizada fornece a capacidade de participação de todas as partes na cadeia de abastecimento. A sua natureza imutável e baseada em criptografia dá a garantia de segurança [6][197]. Estas razões levam a tecnologia *blockchain* a ser aplicada na área de logística e cadeia de abastecimento.

## 4.2. RELAÇÃO ENTRE A TECNOLOGIA BLOCKCHAIN E SUPPLY CHAIN

Um dos objetivos desta dissertação, é entender de que forma a tecnologia *blockchain* está relacionada com a cadeia de abastecimento (*supply chain*) e logística.

Conceptualmente, a coerência da *blockchain* é garantida através da obtenção de consenso descentralizado e consistência nas transações. Os registos provenientes de operações logísticas são igualmente consistentes e datados. Este ponto em comum faz parecer desnecessário o envolvimento de um mediador confiável na manutenção dos registos e operações [48].

Na literatura científica, vários estudos foram feitos acerca da relação entre a tecnologia blockchain e a cadeia de abastecimento:

- *Kshetri* [178], usou um método de casos de estudo para investigar o impacto da *blockchain* em vários objetivos referentes à gestão da cadeia de abastecimento, onde, para cada objetivo foram apresentados casos de sucesso da indústria;
- *Saberi et al*. [198], explora as principais barreiras para a adoção de *blockchains* e, especialmente, *Smart Contracts* para cumprir as metas de gestão da cadeia de abastecimento sustentável;
- *Babich* e *Hilary* [199], fornecem uma revisão abrangente dos estudos de *blockchain* em operações e gestão da cadeia de abastecimento, assim como, a potencial aplicação da tecnologia neste campo, incluindo gestão de inventário, agregação de dados, contratação, gestão de risco da cadeia de abastecimento e cadeia de abastecimento sustentável;

Artigos da indústria e de liderança de pensamento publicados por firmas de consultoria de alto nível, como McKinsey [18], Deloitte [200][187] e Ernst and Young [201] estão, igualmente, a abrir caminho para académicos e profissionais no mundo da tecnologia blockchain [61].

Instalações e parceiros comerciais geograficamente dispersos, geralmente levam a incoerências e complexidade entre os atores da cadeia de abastecimento. Portanto, adquirir e manter dados fidedignos é fundamental. Neste contexto, o objetivo da tecnologia *blockchain* é fornecer redes contínuas, visibilidade total e informações simétricas para todos [4].

Se definirmos cadeia de abastecimento como, "a rede de organizações que estão envolvidas, através de ligações e interações, nos diferentes processos e atividades que produzem valor sobre a forma de produtos e serviços nas mãos do cliente final" [6], podemos verificar que a *blockchain* tem potencial para melhorar a visibilidade, otimização de processos e nivelamento de procura [42]. No entanto, existem ainda limitações inerentes à tecnologia. Apesar dos benefícios propostos pelo conceito de *blockchain* encaixarem de forma integrada nas necessidades da área de cadeia de abastecimento e

logística, a sua implementação ainda não é tão transparente e suave quanto é necessária [4][6][18][48].

## 4.3. BENEFÍCIOS DA TECNOLOGIA BLOCKCHAIN

Os processos da cadeia de abastecimento e logística podem ser melhorados significativamente com a introdução da tecnologia *blockchain*. O registo da transferência de produtos num ledger como transações permite identificar os principais dados relevantes para a gestão da cadeia de abastecimento [6], permitindo que várias partes interessadas da cadeia de abastecimento façam transações entre si sem a necessidade de um intermediário [4].

A tecnologia *blockchain* é considerada uma solução para conectar e gerir dispositivos IoT de forma fiável. A área de *supply chain* e logística é uma das áreas mais promissoras devido à quantidade de possibilidades existentes em ambiente logístico [6][202]. A tecnologia *blockchain* pode melhorar as operações logísticas, reduzindo ou eliminando erros e fraude, minimizando custos, reduzindo desperdício e atrasos, assim como melhorando a gestão de inventário. Esta tecnologia pode estimular as tarefas logísticas no âmbito do rastreamento de pedidos, alterações de pedidos/encomendas e guias de transporte, assim como na partilha de informações e controlo do processo de conceção e entrega de produtos [6].

Alguns pontos concretos são [203]:

- Rastreamento de origem - A falta de transparência leva a problemas de custo e relacionamento com o cliente que podem acabar por denegrir o nome da marca. Na gestão de uma cadeia de abastecimento com recurso a *blockchain*, a manutenção de registos e o rastreamento de origem tornam-se fáceis, pois as informações do produto podem ser acedidas com a ajuda de sensores embutidos (por exemplo: *data loggers*) e/ou etiquetas RFID;
- Redução de custos - O rastreamento em tempo real de um produto numa cadeia de abastecimento com recurso a *blockchain* reduz o custo geral referente à movimentação de itens entre os diferentes nós da cadeia de abastecimento. Quando a *blockchain* é aplicada para agilizar os processos administrativos nas

cadeias de abastecimento, os custos extras que ocorrem no sistema são reduzidos automaticamente, garantindo a segurança das transações;

- Confiança - Ter confiança em cadeias de abastecimento complexas com muitos participantes é necessário para garantir a suavidade das operações. A natureza imutável da *blockchain* na cadeia de abastecimento é bem projetada para evitar adulterações e garantir a confiança na rede.

Um dos benefícios mais atraentes do uso da *blockchain* para dados é que a tecnologia permite que os dados sejam mais interoperáveis. Desta forma, torna-se mais fácil para as empresas partilhar informações e dados com fabricantes, fornecedores e vendedores. A transparência da *blockchain* ajuda a reduzir atrasos e disputas, evitando que os produtos fiquem presos na cadeia de abastecimento. Como cada produto pode ser rastreado em tempo real, as hipóteses de extravio são raras. A tecnologia *blockchain* oferece escalabilidade através da qual qualquer grande base de dados pode ser consultada de vários locais ao redor do mundo [203].

O valor de adotar a tecnologia *blockchain* pode ser tirado do potencial de conectar diferentes pontos de dados enquanto mantém a integridade dos dados entre vários participantes. As propriedades de transparência e imutabilidade da tecnologia *blockchain* tornam-na útil para eliminar fraudes na cadeia de abastecimento e manter a integridade do sistema. Outros benefícios podem ser considerados [203]:

- Reduzir ou eliminar fraudes e erros;
- Melhorar a gestão de *stocks*;
- Minimizar os custos de transporte;
- Reduzir atrasos na papelada;
- Identificar problemas mais rapidamente;
- Aumentar a confiança do consumidor e das diferentes partes interessadas.

## 4.4. IMPLEMENTAÇÃO DE BLOCKCHAIN NA SUPPLY CHAIN

Na adoção de tecnologia *blockchain* para a área de *supply chain* e logística, as empresas devem iniciar com a decisão sobre o tipo de *blockchain ledger* que vão utilizar [18]. Ou seja, *permissioned* ou *permissionless ledger* (discutido no capítulo 2.3.6.).

Uma *framework* que pode ser considerada no desenho da implementação de tecnologia *blockchain* no âmbito industrial, foi apresentada por Petri Helo e Yuqiuge Hao [48]. Este modelo apresenta quatro camadas de arquitetura de sistema conforme ilustrado na Figura 15.

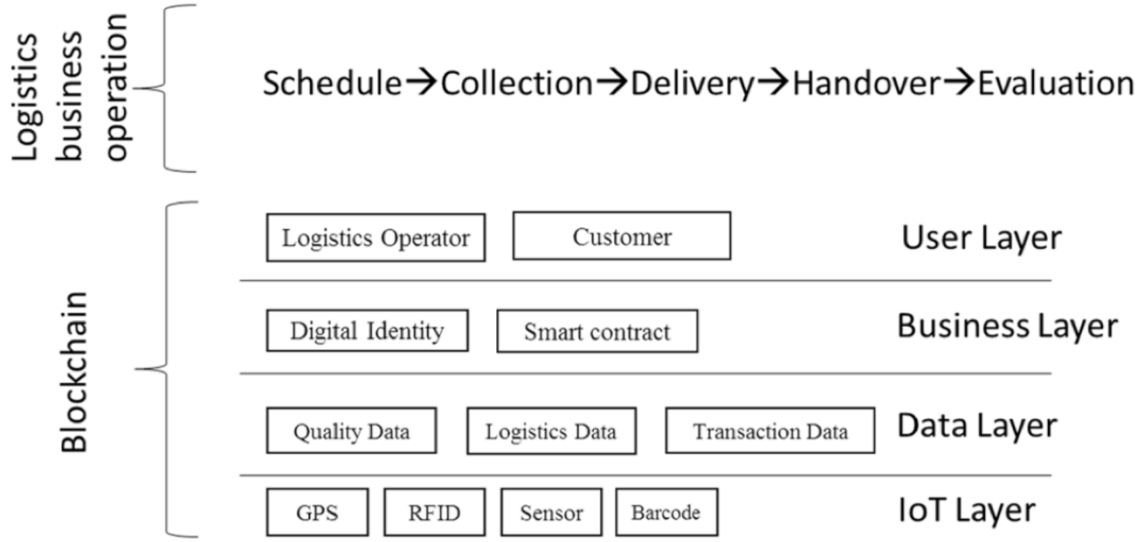


**Figura 15 -** Modelo apresentado por Petri Helo e Yuqiuge [48]

A primeira camada apresentada é a camada de IoT: esta componente do modelo é responsável pela recolha de dados em tempo real. Uma vez que o *ledger* guarda os dados, é necessário garantir que estes são recolhidos de fontes fidedignas [48].

A camada acima corresponde à camada de informação: Nesta fase, os autores distinguem três tipos de informação, (i) informação de qualidade, (ii) informação logística e (iii) informação de transações. Neste ponto, todos os parceiros e partes envolvidas na rede e cadeia de abastecimento guardam uma cópia da informação do *ledger* [48].

A terceira camada trata a componente do negócio. Aqui, a informação é recolhida e partilhada através da camada de informação. Esta categoria do modelo apresentado refere-se às especificidades de cada parte envolvida na rede, estando associado o uso de *smart contracts* [48].

A camada de topo é a camada centrada no utilizador. Esta camada inclui diversos utilizadores da *blockchain* que, tendo permissões, podem monitorizar a qualidade da informação e executar diversas atividades com recurso à *blockchain* [48]. Estas diversas

camadas apresentadas para implementação da *blockchain* na *supply chain* e logística, visam apoiar as operações e tomadas de decisão dos negócios onde são aplicadas.

Ainda no âmbito da implementação de tecnologia *blockchain*, apesar das vantagens, Du Wenyu et al. [204] sugerem três regras a considerar antes de implementar *blockchain*:

(i) Considerar mudanças incrementais ao invés de mudanças disruptivas e radicais na operação;
(ii) Evitar *use-cases* com grandes quantidades de informação, uma vez que pode reduzir a eficiência da *blockchain*;
(iii) Criar um projeto piloto para entender e estudar os riscos inerentes da tecnologia *blockchain* [61][204].

A literatura da cadeia de abastecimento está particularmente interessada na tecnologia *blockchain* como uma forma de permitir que organizações e indivíduos façam e verifiquem transações sem a necessidade de uma autoridade central [4].

## 4.5. BLOCKCHAIN LEDGER NA SUPPLY CHAIN

Outro objetivo deste trabalho é identificar qual o *blockchain ledger* mais adequado para aplicações na área de cadeia de abastecimento (*supply chain*) e logística.

No subcapítulo anterior foi identificado um modelo apresentado por Petri Helo e Yuqiuge Hao [48] assente em quatro camadas de implementação da tecnologia. No trabalho de Du Wenyu et al. [204], são sugeridas três regras a considerar aquando o desenvolvimento de uma solução na área de *supply chain* [61][204]. Acrescentar que, para cenários em ambiente volátil e ágil, blockchains privadas e customizadas funcionam melhor [4].

A relação entre *blockchain ledgers* e *supply chain* acaba por ter uma abrangência conceptual grande, resumindo-se efetivamente a dois *ledgers*, *Hyperledger* [129][130][131][205] e *Ethereum* [4]. Neste tópico, percebemos que os ledgers mais utilizados e com provas de conceito bem sucedidas, estão assentes no *Hyperledger Fabric* [107], no *Hyperledger Sawtooth* [121] e na *Ethereum* [88][134][143].

### 4.5.1. HYPERLEDGER FABRIC

O *Hyperledger Fabric* é uma plataforma *distributed ledger technology* (DLT) *open-source*, projetada para uso em contextos empresariais [206][207]. Um dos aspetos positivos desta plataforma é a sua modularidade. Numa explicação de alto nível, podemos enumerar alguns módulos constituintes da plataforma [207]:

- Um serviço de pedidos que estabelece consenso sobre a ordem das transações e, em seguida, transmite os blocos aos diferentes nós da rede;
- Um provedor de serviços de associação que é responsável por associar entidades na rede a identidades criptográficas;
- Um serviço opcional ponto a ponto que dissemina a saída dos blocos solicitando serviço a outros pares;
- *Smart Contracts* ("*chaincode*") executados em ambiente de *container* (por exemplo, *Docker*). Podem ser escritos em linguagens de programação padrão, mas não têm acesso direto ao estado do *ledger*.
- O *ledger* pode ser configurado para suportar uma variedade de Sistemas de Gestão de Base de Dados (SGBD);
- Uma aplicação de política de endereçamento e validação que pode ser configurada por aplicativo de forma independente.

O *Hyperledger Fabric* é uma *blockchain* privada e do tipo *permissioned* [207]. Os componentes principais deste *ledger* são [206]:

- *Assets — Assets* podem variar desde tangíveis (imóveis e hardware) até intangíveis (contratos e propriedade intelectual). O *Hyperledger Fabric* oferece a capacidade de modificar *assets* usando transações do *chaincode*. São representados como uma coleção de pares de valores-chave, com mudanças de estado registadas como transações num *ledger*.
- *Chaincode – Chaincode* define um *asset* ou conjunto de *assets* e as instruções de transação para a respetiva modificação. Em suma, é a lógica do negócio. *Chaincode* impõe as regras para ler ou alterar pares de valores-chave ou outras informações. As funções *Chaincode* são executadas na base de dados do estado atual do *ledger* e são iniciadas por meio de uma proposta de transação.

- Privacidade – Permitem transações multilaterais privadas e confidenciais que geralmente são exigidas por empresas concorrentes e setores regulamentados que trocam *assets* numa rede comum.
- Segurança – O facto de ser uma *blockchain* do tipo *permissioned* torna o *Hyperledger Fabric* numa rede confiável, onde os participantes sabem que todas as transações podem ser detetadas e rastreadas por reguladores e auditores autorizados.
- *Consensus* – Uma abordagem diferente de consenso permite a flexibilidade e escalabilidade necessárias para o desenvolvimento empresarial.

O funcionamento de uma aplicação do *Hyperledger Fabric* pode ser demonstrado através da Figura 16.

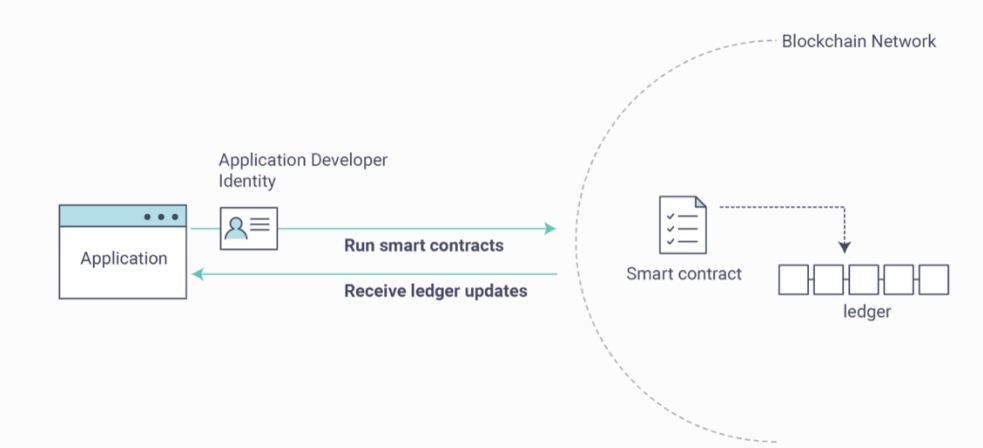


**Figura 16** - Funcionamento de uma aplicação no *Hyperledger Fabric* [206]

O esquema representa uma rede *blockchain Fabric* que contém *Smart Contracts*. A aplicação interage com a rede garantindo a verificação da identidade do nó na rede, de forma a correr os *Smart Contacts* existentes. Quando os *Smart Contracts* são executados, enviam atualizações de estado para os nós da rede, atualizando o *ledger*. Estas atualizações são vistas na aplicação [206][207].

### 4.5.2. HYPERLEDGER SAWTOOTH

O *Hyperledger Sawtooth* é outra plataforma *distributed ledger technology* (DLT) *open-source*, projetada para uso em contextos empresariais [208]. Uma das diferenças face ao *Hyperledger Fabric* é a separação entre o nível aplicacional e o *core system* da *blockchain*

[121]. O esquema de funcionamento do *Hyperledger Sawtooth* é apresentado na Figura 17 [208].

Com base na arquitetura do sistema, podemos identificar os componentes principais do *Sawtooth* [208]:

- *Validator Node* – Composto por uma API REST, um *validator*, um *consensus engine* e um ou mais *transaction processors*;
- API REST – É o componente central que adapta a comunicação com um *validator* aos padrões HTTP/JSON;
- *Validator* – Componente responsável por validar lotes de transações, transformando os lotes em blocos. Responsável por manter o consenso com a rede *Sawtooth* e a coordenação da comunicação entre clientes, *transaction processors* e outros *validators* da rede;
- *Consensus Engine* – Componente que fornece a funcionalidade específica de consenso para um nó *Sawtooth*. O mecanismo de consenso é executado como um processo separado no nó e comunica com o *validator* por meio da API de consenso;
- *Transaction Processor* – Valida as transações e atualiza o estado com base nas regras definidas pela família de transações associada;
- *Sawtooth Network* – Rede distribuída ponto a ponto de nós executando um *validator* (e componentes associados) que trabalham no mesmo *blockchain ledger*.

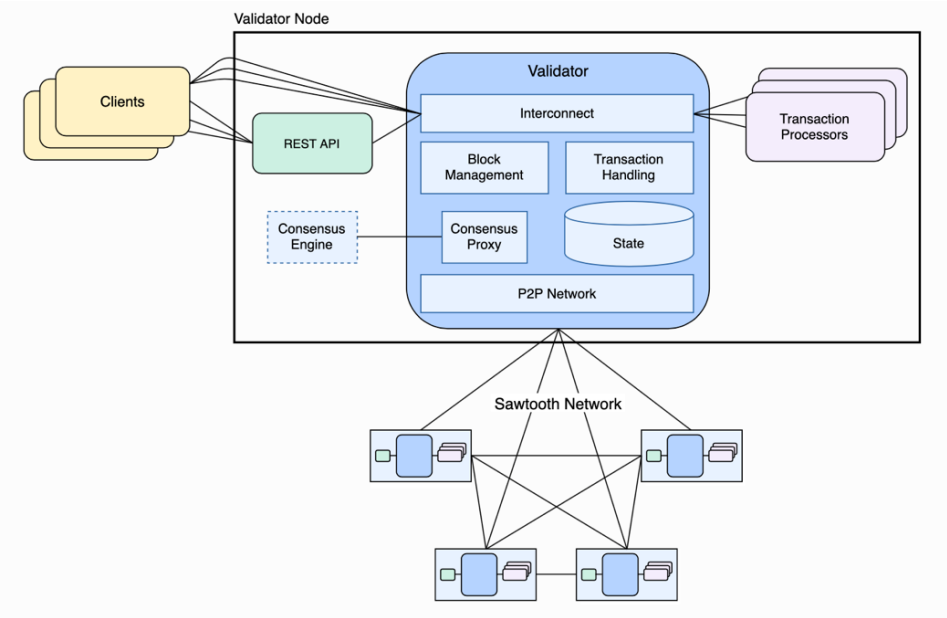


**Figura 17** - Arquitetura do sistema *Hyperledger Sawtooth* [208]

O *Hyperledger Sawtooth*, para além da separação entre a componente de desenvolvimento aplicacional e o *core system*, permite uma execução paralela de transações na rede. Está igualmente preparado para *broadcast* de eventos na rede entre diferentes *assets*, e garante compatibilidade com *Smart Contracts Ethereum* [121][208].

Uma das funcionalidades existentes é o *consensus* dinâmico na rede [121]. Este modelo pode ser alterado com a rede em pleno funcionamento, dependendo das necessidades atuais. O *Sawtooth* permite o uso de algoritmos como PBFT [89][208] e PoET [119], entre outros.

### 4.5.3. ETHEREUM

*Ethereum* oferece acesso aberto a dinheiro digital, criptomoedas, e serviços de dados para todos – não importa a origem ou localização. É uma tecnologia desenvolvida pela comunidade por trás da criptomoeda *Ether* (ETH) [209].

A intenção da *Ethereum* é criar um protocolo alternativo para a construção de aplicações descentralizadas, fornecendo um conjunto diferente de vantagens, com destaque particular em situações para o tempo de desenvolvimento rápido, segurança para pequenas aplicações raramente usados e a capacidade de aplicações diferentes interagirem de forma muito eficiente [143].

Na *Ethereum*, o estado da *blockchain* é composto por objetos chamados "contas", com cada conta tendo um endereço de 20 bytes e as transições de estado sendo transferências diretas de valor e informações entre contas [209]. Uma conta *Ethereum* contém quatro campos:

(i) O *nonce*, um contador usado para garantir que cada transação só possa ser processada uma vez;
(ii) O saldo atual da conta;
(iii) O código do contrato da conta (se houver);
(iv) O armazenamento da conta (vazio por padrão).

A Figura 18 mostra a função de transição de estado *Ethereum*, que pode ser definida através dos seguintes passos [209]:

(i) Verificar se a transação está bem formada (ou seja, tem o número certo de valores), a assinatura é válida e o *nonce* corresponde ao *nonce* na conta do remetente. Caso contrário, retornar um erro;
(ii) Calcular a taxa de transação como e determinar o endereço de envio a partir da assinatura. Subtrair a taxa do saldo da conta do remetente e aumentar o *nonce* do remetente. Se não houver saldo suficiente para gastar, retornar um erro;
(iii) Transferir o valor da transação da conta do remetente para a conta de receção. Se a conta de receção ainda não existir, criar. Se a conta de receção for um contrato, executar o código do contrato até a conclusão ou até que o gás da execução acabe;
(iv) Se a transferência do valor falhou porque o remetente não tinha dinheiro suficiente ou a execução do código ficou sem gás, reverter todas as alterações de estado, exceto o pagamento das taxas, e adicionar as taxas à conta do *miner*;
(v) Caso contrário, devolver as taxas de todo o gás restante ao remetente e enviar as taxas pagas pelo gás consumido ao *miner*.

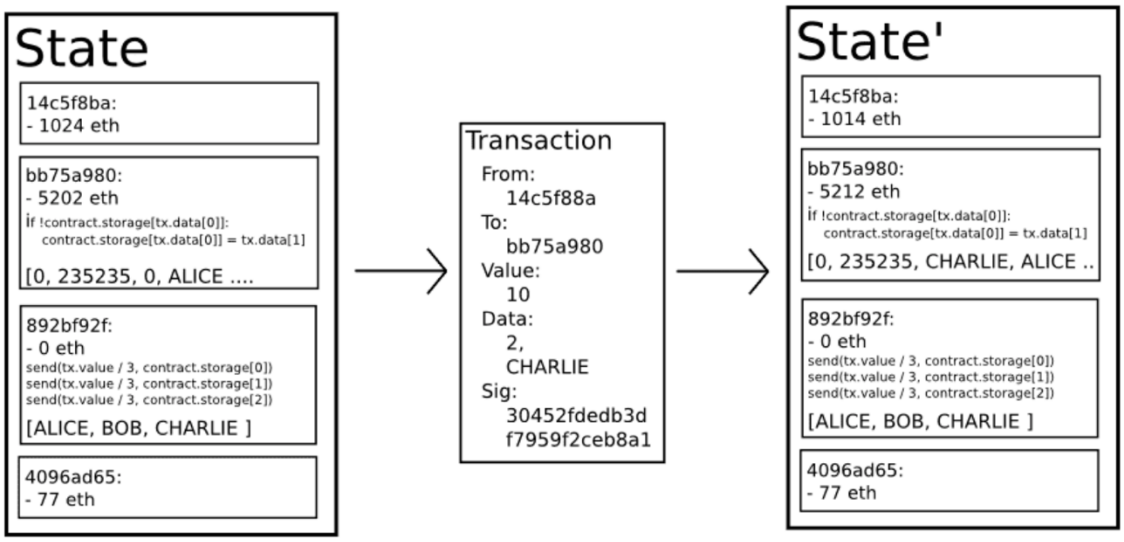


**Figura 18** - Função de transição de estado *Ethereum* [209]

## 4.6. DÚVIDAS SOBRE A TECNOLOGIA BLOCKCHAIN

Uma das limitações que é destacada em diferentes estudos, é a *performance* da tecnologia *blockchain* [6]. A tecnologia carece de um consumo elevado de energia e poder de processamento, levantando preocupações ambientais [4]. Apesar das diferentes iterações e novos algoritmos de *consensus* criados, a *blockchain* ainda está situada numa fase de imaturidade [210]. A não existência de standards ou legislação, dificulta a sua implementação e adoção [210].

O grau de exigência da tecnologia pode levar a que algumas empresas não invistam nesta área, de modo a não arriscarem os modelos de negócio existentes [4]. O facto de, a tecnologia *blockchain* assentar na transparência dos dados e validação de identidade, pode levar a que empresas não queiram partilhar informações sobre uma tecnologia que ainda não se encontra totalmente desenvolvida [211][212].

De forma a garantir que uma rede *blockchain* consegue operar numa cadeia de abastecimento, é necessário garantir que todos os intervenientes estejam ligados na mesma *blockchain*. Esta questão levanta problemas ao nível da interoperabilidade de sistemas e transferência de dados entre os diferentes nós da rede [4].

Atualmente, o uso de tecnologia *Blockchain* para a implementação de *distributed ledgers*, resolve tantos problemas como aqueles que levanta [4]. O período de desenvolvimento de soluções assentes nesta tecnologia e capazes de serem escaláveis e práticas é longo. O custo de mão de obra especializada nesta área e formação necessária são de alto nível de investimento [48]. Vários projetos iniciais falharam a escalabilidade da solução proposta. No ano de 2016, apenas 8% de um universo de 26.000 projetos na área de *Blockchain* apresentaram resultados positivos e sucesso [61][213].

Em suma, a adoção da tecnologia *Blockchain* tem um caminho longo a percorrer. Somente quando existirem cadeias de abastecimento massivas a utilizar esta tecnologia e legislação que suporte o apoio, ou compreensão, governamental é que poderemos esperar um crescimento significativo desta tecnologia na área logística empresarial [18][48].

# 5. APLICAÇÃO PRÁTICA DE CONCEITOS

Este capítulo irá simular a inicialização, criação e interação de uma instância do *Hyperledger Fabric* entre dois nós da rede (*peers*). O objetivo é demonstrar os conceitos práticos de utilização deste *ledger* e o funcionamento da tecnologia *blockchain*.

Cada vez mais, a rastreabilidade de componentes críticos entre fornecedores e indústria de manufatura é imposta. No setor automóvel, peças críticas têm como, entre outros, requisitos de rastreabilidade para cada posto de trabalho [214]. Neste caso, o cliente pretende saber por onde aquela peça passou durante o seu processo de fabrico. Ao imaginarmos o desenvolvimento de um automóvel, podemos identificar peças críticas no mesmo. Estas peças, seguem diretivas rígidas antes, durante e após a sua criação [215].

A título exemplificativo, irá ser utilizada linguagem relacionada com a cadeia de abastecimento nesta área. Teremos duas empresas pertencentes à mesma rede *blockchain*, na qual terão acesso a ver as peças críticas, algumas características e o stock de ambas. Este exemplo prático demonstra a transparência, imutabilidade e veracidade do uso de tecnologia *blockchain*. Podemos extrapolar este caso para uma relação de cliente/fornecedor, onde o cliente pretende saber em tempo real e de forma confiável, quantas peças críticas tem o fornecedor neste momento e o seu estado de desenvolvimento.

## 5.1. TECNOLOGIA UTILIZADA

As ferramentas chave utilizadas para este caso prático foram:

- O *Hyperledger Fabric*, que serviu de base à criação de uma rede *blockchain*. Foi utilizada esta Framework devido à sua modularidade e funcionamento;

- O *Docker* foi utilizado de forma a virtualizar as organizações pertencentes à rede. Esta virtualização acontece por meio de *containers* que, nada mais são do que repositórios virtuais isolados entre si e que agrupam o próprio software, bibliotecas e arquivos de configuração;
- GO é uma linguagem de programação desenvolvida pela Google e utilizada para a criação do *Smart Contract* apresentado.

## 5.2. INICIALIZAÇÃO DA BLOCKCHAIN

O primeiro passo para o desenvolvimento do caso prático é a inicialização da *blockchain*. Uma vez que a base será assente no *Hyperledger Fabric* [206], é necessária a instalação dos componentes básicos do *ledger* escolhido. A Figura 19 mostra os componentes instalados para a versão 1.4.9 do *Hyperledger Fabric*.

```
===> Pulling fabric ca Image
====> hyperledger/fabric-ca:1.4.9
1.4.9: Pulling from hyperledger/fabric-ca
Digest: sha256:28f50c6aa4f4642842e706d3ae6dcee181921d03bd30ab2a8b09b66e0349d92f
Status: Image is up to date for hyperledger/fabric-ca:1.4.9
docker.io/hyperledger/fabric-ca:1.4.9
===> List out hyperledger docker images
hyperledger/fabric-ca                      1.4                 dbbc768aec79        4 weeks ago         158MB
hyperledger/fabric-ca                      1.4.9               dbbc768aec79        4 weeks ago         158MB
hyperledger/fabric-ca                      latest              dbbc768aec79        4 weeks ago         158MB
hyperledger/fabric-tools                   2.2                 e9b802fadb41        4 weeks ago         519MB
hyperledger/fabric-tools                   2.2.1               e9b802fadb41        4 weeks ago         519MB
hyperledger/fabric-tools                   latest              e9b802fadb41        4 weeks ago         519MB
hyperledger/fabric-peer                    2.2                 ece149884124        4 weeks ago         55MB
hyperledger/fabric-peer                    2.2.1               ece149884124        4 weeks ago         55MB
hyperledger/fabric-peer                    latest              ece149884124        4 weeks ago         55MB
hyperledger/fabric-orderer                 2.2                 78a16ddd2cf4        4 weeks ago         38.4MB
hyperledger/fabric-orderer                 2.2.1               78a16ddd2cf4        4 weeks ago         38.4MB
hyperledger/fabric-orderer                 latest              78a16ddd2cf4        4 weeks ago         38.4MB
hyperledger/fabric-ccenv                   2.2                 8e554c280cac        4 weeks ago         586MB
hyperledger/fabric-ccenv                   2.2.1               8e554c280cac        4 weeks ago         586MB
hyperledger/fabric-ccenv                   latest              8e554c280cac        4 weeks ago         586MB
hyperledger/fabric-baseos                  2.2                 0b99d26b26ad        4 weeks ago         6.85MB
hyperledger/fabric-baseos                  2.2.1               0b99d26b26ad        4 weeks ago         6.85MB
hyperledger/fabric-baseos                  latest              0b99d26b26ad        4 weeks ago         6.85MB
hyperledger/grid-dev                       v3                  57b349a53f73        7 weeks ago         1.14GB
hyperledger/sawtooth-sabre-cli             latest              0a0da6b7d5e5        7 weeks ago         169MB
hyperledger/grid-dev                       v2                  1a5b1957d92c        2 months ago        2.45GB
hyperledger/sawtooth-devmode-engine-rust   1.2                 560261e471f9        2 months ago        113MB
hyperledger/sawtooth-validator             1.2                 54cce2fc13a7        4 months ago        294MB
hyperledger/sawtooth-settings-tp           1.2                 88a4a0bace0b        4 months ago        114MB
hyperledger/sawtooth-rest-api              1.2                 b9b045d82534        4 months ago        157MB
hyperledger/sawtooth-sabre-tp              0.5                 281411092cb6        8 months ago        114MB
hyperledger/sawtooth-sabre-cli             0.5                 dbd2aa3adc6e        8 months ago        169MB
hyperledger/sawtooth-validator             1.1                 21768fa6dc88        18 months ago       227MB
hyperledger/sawtooth-shell                 1.1                 840c388b2f10        18 months ago       188MB
hyperledger/sawtooth-settings-tp           1.1                 ef4777febc35        18 months ago       168MB
hyperledger/sawtooth-rest-api              1.1                 2a3050476952        18 months ago       174MB
hyperledger/sawtooth-devmode-engine-rust   1.1                 f3fa908cc49c        18 months ago       125MB
```

**Figura 19** - Componentes *Hyperledger Fabric* instalados

Conforme descrito anteriormente, de forma a trabalhar com os componentes instalados, foi necessário configurar o *Docker* para trabalhar simular o caso prático apresentado. A Figura 20 mostra a execução de três *containers*:

- *Orderer* - Cada rede *Fabric* inclui um serviço de pedidos. Embora os *peers* validem as transações e adicionem blocos de transações ao *ledger*, estes não decidem a ordem das transações nem são responsáveis pela inclusão das transações em novos blocos. Numa rede distribuída, os *peers* podem estar longe uns dos outros e não ter uma visão comum de quando uma transação foi criada. Chegar a um consenso sobre a ordem das transações é um processo caro que criaria sobrecarga para os diversos *peers*. Um serviço de pedidos permite que os *peers* concentrem os seus esforços na validação e confirmação de transações no *ledger*. Este *orderer* usa um serviço de pedidos *Raft*.
- *Peer* - Os *peers* armazenam o *ledger* da *blockchain* e validam as transações antes de serem confirmadas no *ledger*. Os *peers* executam os *Smart Contracts* que contêm a lógica de negócios que é usada para gerir os ativos no *ledger*. Cada *peer* na rede precisa de pertencer a um consórcio (Consortium). A título exemplificativo, estão criados dois *consortiums*.


**Figura 20** - *Docker Containers* para o caso prático

Apesar de existirem dois *peers* (doravante chamados empresas) criados, estes não conseguem comunicar entre si. Isto acontece devido ao facto do anonimato na rede. A empresa A só consegue comunicar com a empresa A se houver consentimento e for criado um canal de comunicação entre ambas, sendo este canal oculto para as restantes empresas da rede (*peers*).

A Figura 21 mostra que os *peers* e o serviço de pedidos – *orderer* – estão a ser executados no *Docker*.

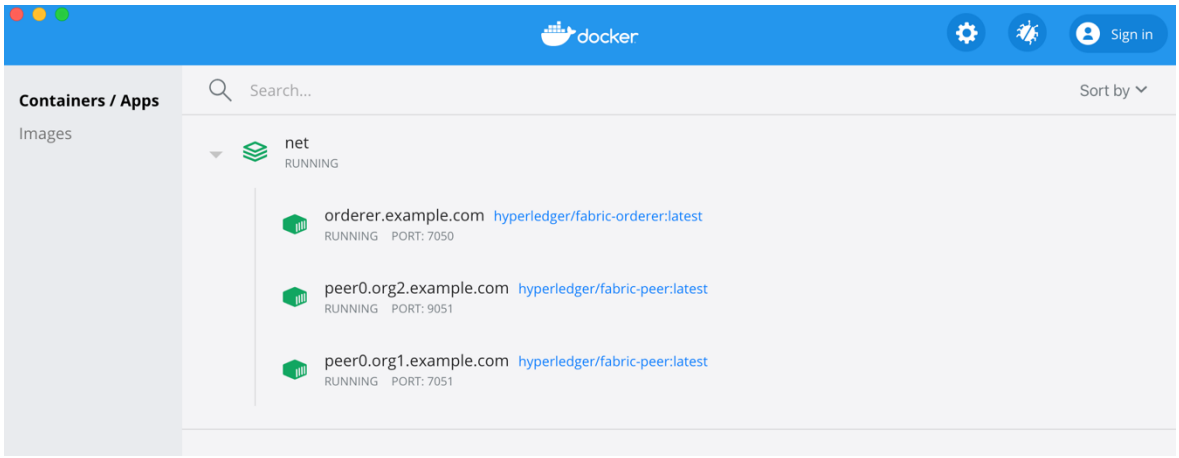


**Figura 21** - *Containers* em execução no *Docker*

De forma a tornar a escrita mais compreensível, doravante o *peer0.org1* será a empresa cliente do nosso caso e o *peer0.org2* será a empresa fornecedor.

## 5.3. CRIAÇÃO DE UM CANAL DE COMUNICAÇÃO

Conforme referido anteriormente, é necessária a criação de um canal de comunicação entre o cliente e o fornecedor para que estes possam partilhar da mesma informação e manterem, em conjunto, a mesma versão do *ledger*. Os canais de comunicação do *Fabric* são uma camada de comunicação privada entre membros específicos da rede. Estes podem ser utilizados por organizações convidadas para o canal e são invisíveis para os outros membros da rede [206].

Cada canal de comunicação possui um *ledger* separado. As organizações pertencentes ao canal, armazenam e mantêm a mesma cópia do mesmo e são responsáveis por validarem em conjunto as transações no canal de comunicação. A Figura 22 mostra a criação do canal "pecas.criticas" entre o peer0.org1 e o peer0.org2, neste contexto, entre cliente e fornecedor.

```
Channel 'pecas.criticas' created
Join Org1 peers to the channel...
Using organization 1
+ peer channel join -b ./channel-artifacts/pecas.criticas.block
+ res=0
2020-10-31 16:36:51.843 WET [channelCmd] InitCmdFactory -> INFO 001 Endorser and orderer connections initialized
2020-10-31 16:36:51.889 WET [channelCmd] executeJoin -> INFO 002 Successfully submitted proposal to join channel
Join Org2 peers to the channel...
Using organization 2
+ peer channel join -b ./channel-artifacts/pecas.criticas.block
+ res=0
2020-10-31 16:36:54.985 WET [channelCmd] InitCmdFactory -> INFO 001 Endorser and orderer connections initialized
2020-10-31 16:36:55.029 WET [channelCmd] executeJoin -> INFO 002 Successfully submitted proposal to join channel
```

**Figura 22** - Criação do canal de comunicação "pecas.criticas"

O nome do canal não pode conter caracteres especiais ou letras maiúsculas. A sua criação necessita que ambos o membros pertençam à mesma rede.

O que acontece é um pedido ao *endorser* para que seja criado um canal de comunicação entre dois membros. De seguida, validando os requisitos para a criação do canal, o *endorser* envia um pedido a cada um dos membros em questão para que estes aceitem, ou não, fazerem parte do mesmo canal de comunicação. Sendo positivo, ambos os *peers* dos membros propostos, são colocados no mesmo canal de comunicação. De notar que, os membros em questão são *consortiums*, ou seja, conjuntos de *peers*. No caso apresentado cada *consortium* contempla apenas um peer.

## 5.4. SMART CONTRACTS E CHAINCODE

Depois da criação do canal de comunicação entre o cliente e o fornecedor, é necessária a criação de *Smart Contracts* para interação com o *ledger* do canal. Os *Smart Contracts* contemplam a lógica de negócios que irá governar os ativos no *ledger* da *blockchain*. Desta forma, é possível que os membros do canal criem, alterem ou transfiram os ativos correspondentes, neste caso, peças críticas, entre eles [107].

No *Fabric*, os *Smart Contracts* são implementados na rede em pacotes chamados de *chaincode*. Um *Chaincode* é instalado nos *peers* de uma organização e, em seguida, implantado num canal, onde pode ser usado para transmitir transações e interagir com o *ledger*. Antes que um *chaincode* possa ser implementado num canal, os membros do canal precisam de concordar com uma definição de *chaincode* que estabelece o modelo de gestão do *chaincode*. Quando o número necessário de organizações concorda, a definição do *chaincode* pode ser confirmada para o canal e o *chaincode* está pronto para ser usado

[107]. A Figura 23 mostra a concordância entre as duas organizações para implementação do *chaincode* desenvolvido.

```
Chaincode definition approved on peer0.org2 on channel 'pecas.criticas'
Using organization 1
Checking the commit readiness of the chaincode definition on peer0.org1 on channel 'pecas.criticas'...
Attempting to check the commit readiness of the chaincode definition on peer0.org1, Retry after 3 seconds.
+ peer lifecycle chaincode checkcommitreadiness --channelID pecas.criticas --name basic --version 1.0 --sequence 1 --output json
+ res=0
{
        "approvals": {
                "Org1MSP": true,
                "Org2MSP": true
        }
}
Checking the commit readiness of the chaincode definition successful on peer0.org1 on channel 'pecas.criticas'
Using organization 2
Checking the commit readiness of the chaincode definition on peer0.org2 on channel 'pecas.criticas'...
Attempting to check the commit readiness of the chaincode definition on peer0.org2, Retry after 3 seconds.
+ peer lifecycle chaincode checkcommitreadiness --channelID pecas.criticas --name basic --version 1.0 --sequence 1 --output json
+ res=0
{
        "approvals": {
                "Org1MSP": true,
                "Org2MSP": true
        }
}
Checking the commit readiness of the chaincode definition successful on peer0.org2 on channel 'pecas.criticas'
```

**Figura 23** - Aceitação do *chaincode* por parte das organizações do canal

No *Docker* é possível visualizar a instância do *chaincode* do canal entre as organizações. A Figura 24 mostra as instâncias do *chaincode* instalado para a *org1* e a *org2* – *dev-peer.org1* e *dev-peer.org2* respetivamente.

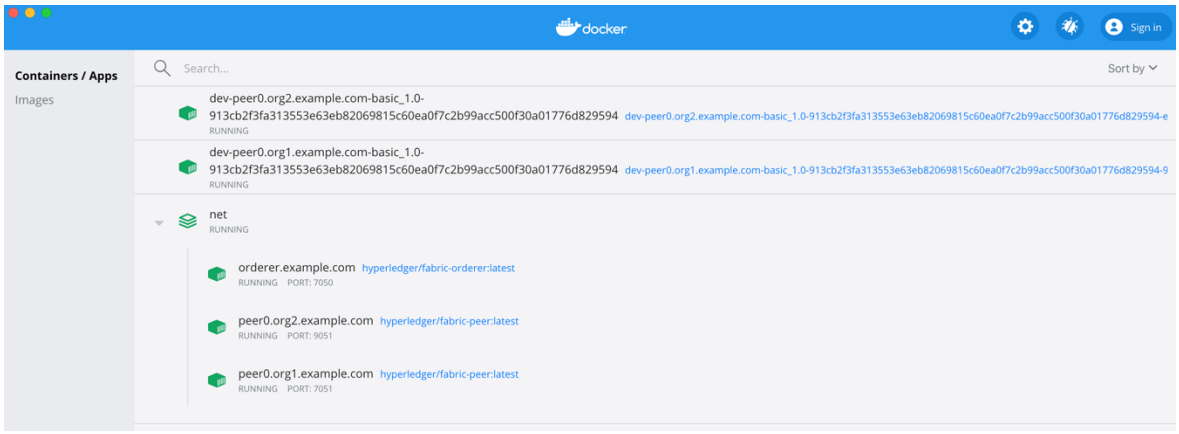


**Figura 24** - Instância de *chaincode* no *Docker*

## 5.5. USABILIDADE DO LEDGER

Ao iniciar o *chaincode*, irão ser criados alguns registos iniciais. A Figura 25 mostra os dados do *ledger*.

[{"ID":"material1","color":"azul","size":10,"owner":"Empresa1","appraisedValue":300},{"ID":"material2","color":"vermelho","size":5,"owner":"Empresa1","appraisedValue":400},{"ID":"material3","color":"verde","size":10,"owner":"Empresa2","appraisedValue":500},{"ID":"material4","color":"amarelo","size":10,"owner":"Empresa2","appraisedValue":600},{"ID":"material5","color":"preto","size":15,"owner":"Empresa1","appraisedValue":700},{"ID":"material6","color":"branco","size":15,"owner":"Empresa2","appraisedValue":800}]

**Figura 25** - Dados iniciais do *ledger*

Estes registos foram criados com recurso à função "*InitLedger*", apresentada anteriormente. É possível ver que o material 6 é branco, pertence ao fornecedor (Empresa2) e este tem 15 unidades.

A criação de novos materiais pode ser feita com recurso à função "*CreateAsset*". A Figura 26 mostra o log da criação de um novo registo no *ledger* através do *orderer*.

```
2020-10-31 17:38:04.463 UTC [orderer.consensus.etcdraft] propose -> INFO 07d Created block [7], there are 0 blocks in flight
channel=pecas.criticas node=1
2020-10-31 17:38:04.475 UTC [orderer.consensus.etcdraft] writeBlock -> INFO 07e Writing block [7] (Raft index: 9) to ledger
channel=pecas.criticas node=1
```

**Figura 26** - Criação de um bloco na rede (ficheiro log do *Docker* - *orderer peer*)

Ao ser criado o bloco número 7, podemos pesquisar por ele dentro da rede e obter o seu estado atual. A Figura 27 mostra o output da função "*ReadAsset*" para o bloco recém-criado.

{"ID":"material7","color":"laranja","size":30,"owner":"Empresa1","appraisedValue":400}

**Figura 27** - Estado atual do material 7

Ao verificar o estado atual da rede, conseguimos obter a informação da *hash* atual e da anterior. Para validar a questão de segurança e funcionamento da *blockchain*, a Figura 28 mostra o valor das *hashes* respetivas.

```
2020-10-31 17:46:59.556 UTC [channelCmd] InitCmdFactory -> INFO 001 Endorser and orderer connections initialized
Blockchain info: {"height":8,"currentBlockHash":"vwF9w5LLqNC+V8iSz+KkJJFrr23WfCNAnk8X3/Nwhaw=","previousBlockHash":"8pytdRIcsjgtyWEpBzgf+nósy/+LGwoFNEYxCWlJubk="}
```

**Figura 28** - Estado da *blockchain*

Verificamos que a *hash* atual é *"vwF9w5LLqNC+V8iSz+KkJJFrr23WfCNAnk8X3/Nwhaw="*. Pelo funcionamento da *blockchain*, aquando a criação do próximo bloco, esta *hash* deve ser utilizada e, por essa razão, indicada como a *hash* anterior. A Figura 29 ilustra este ponto. A criação de um novo bloco – material 9 – originou uma nova *hash*, mas devolveu a anterior em conformidade.

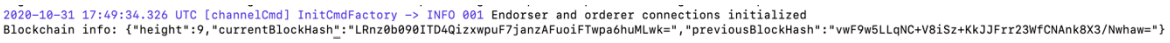


**Figura 29** - Verificação de *hashes* na criação de um novo bloco

Desta forma a rede contém 9 blocos, as *hashes* de cada bloco estão corretas e o funcionamento do *Fabric* permite a interação com o *ledger* através do *Smart Contract* criado.

# 6. CONCLUSÕES

Este capítulo final aborda as conclusões do trabalho de investigação desenvolvido. Inicia com um resumo e exposição das "Principais Conclusões" alcançadas, antes de abordar as "Limitações da Investigação". Termina com indicações para "Trabalho Futuro" e uma introspeção sobre o resultado final atingido.

## 6.1. PRINCIPAIS CONCLUSÕES

A tecnologia *blockchain* tem uma grande correlação com a cadeia de abastecimento e logística [61][187]. Existe potencial para a adoção da tecnologia em prol de benefícios [42]. No entanto, não são lineares os desenvolvimentos e os caminhos necessários para a sua adoção em massa. Existem dúvidas em relação à tecnologia e problemas técnicos que ainda estão por resolver [4][6][18][48]. A falta de legislação ou apoio governamental poderá ser uma barreira na adoção da tecnologia por parte de empresas. Do que foi possível verificar, o desenvolvimento e adoção da tecnologia na *supply chain* deve seguir os seguintes requisitos [206]:

1. Os participantes devem ser identificáveis e identificados;
2. É necessário garantir uma alta taxa de transações;
3. É importante obter baixos valores de latência na confirmação de transações;
4. As redes devem ser do tipo *permissioned*;
5. Deve ser garantida a privacidade e confidencialidade das transações e informação enviada entre nós da rede.

Outro ponto interessante centra-se no facto de os *ledgers* mais utilizados para a *supply chain* e gestão de materiais/bens, serem o *Hyperledger Fabric* o *Hyperledger Sawtooth* e Ethereum. Cada um com as suas especificações, pretendem garantir que os requisitos acima citados são cumpridos [129][130][131][205].

## 6.2. LIMITAÇÕES DA INVESTIGAÇÃO

A investigação levada avante neste trabalho teve uma base em revisões sistemáticas de literatura (SLR) relativas ao tema *blockchain* e *supply chain*. Com esta base, foi possível encontrar artigos citados nas respetivas SLR e abranger mais conteúdo. A web foi igualmente um local onde os conteúdos foram aprofundados, sempre com o objetivo de clarificar o tópico e acrescentar valor ao trabalho final.

No entanto, só foram incluídos artigos publicados em *Journals* até ao primeiro trimestre de 2020 (Março). Esta limitação prevê a perda de alguma informação agregadora mais recente do que a apresentada.

Não foi tido em conta na população inicial, artigos científicos especificamente aplicacionais ou de desenvolvimento de casos práticos. Esta limitação traduz-se num trabalho de conteúdo teórico e conceptual, embora com o desenvolvimento de um capítulo de aplicação prática de conceitos.

## 6.3. TRABALHO FUTURO

No futuro, seria interessante analisar os casos práticos e o desenvolvimento de soluções aplicacionais na área de *supply chain*. Numa tentativa de elevar o trabalho desenvolvido nesta dissertação, poderia ser pertinente entrar a fundo no âmbito arquitetural de uma solução *blockchain* para a cadeia de abastecimento de um determinado setor empresarial.

O desenvolvimento de uma solução ou prova de conceito em ambiente produtivo, seria de enorme valor para provar as bases aqui descritas, relativamente à implementação da tecnologia e aos requisitos para adoção da mesma.

## 6.4. CONCLUSÕES FINAIS

Houve, certamente, durante a leitura desta dissertação, perguntas por responder. No entanto, o objetivo principal considera-se cumprido culminando num estudo aprofundado da tecnologia *blockchain*, com uma visão geral sobre os domínios de aplicação da mesma e as suas especificidades aplicadas na *supply chain*.

O trabalho desenvolvido originou a passagem por diversos conceitos dentro da tecnologia *blockchain*, de modo a ser possível identificar as particularidades desta tecnologia num

mundo diferente das criptomoedas. Foi interessante perceber quais os potenciais problemas que a *blockchain* pode resolver na *supply chain* e perceber de igual forma, quais os problemas existentes para a sua adoção alargada neste meio. Identificar quais os *ledgers* usados e apresentar, ainda que de forma sucinta, o seu funcionamento, foi o resultado alcançado no decorrer deste trabalho.

É válida a assunção de que a tecnologia *blockchain* terá espaço na *supply chain* e logística. Existem desafios de ambas as partes para resolver, antes de a propagação da tecnologia acontecer. No entanto, esta tecnologia abre portas para um futuro promissor e melhor.

# *Referências Documentais*


[1] T. Ko, J. Lee, and D. Ryu, “Blockchain technology and manufacturing industry: Real-time transparency and cost savings,” *Sustain.*, vol. 10, no. 11, Nov. 2018, doi: 10.3390/su10114274.

[2] J. Ream, Y. Chu, and D. Schatsky, “Upgrading blockchains: Smart contract use cases in industry | Deloitte Insights,” *Deloitte*, 2016.

[3] M. Shamout, “Understanding blockchain innovation in supply chain and logisticsindustry,” *Int. J. Recent Technol. Eng.*, vol. 7, no. 6, pp. 616–622, 2019.

[4] Y. Wang, J. H. Han, and P. Beynon-Davies, “Understanding blockchain technology for future supply chains: a systematic literature review and research agenda,” *Supply Chain Management*, vol. 24, no. 1. Emerald Group Publishing Ltd., pp. 62–84, Jan. 14, 2019, doi: 10.1108/SCM-03-2018-0148.

[5] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, “Where is current research on Blockchain technology? - A systematic review,” *PLoS One*, 2016, doi: 10.1371/journal.pone.0163477.

[6] E. Tijan, S. Aksentijević, K. Ivanić, and M. Jardas, “Blockchain technology implementation in logistics,” *Sustainability (Switzerland)*, vol. 11, no. 4. MDPI AG, Feb. 01, 2019, doi: 10.3390/su11041185.

[7] J. Lindman, V. K. Tuunainen, and M. Rossi, “Opportunities and Risks of Blockchain Technologies: A Research Agenda,” in *Proceedings of the 50th Hawaii International Conference on System Sciences (2017)*, 2017, doi: 10.24251/hicss.2017.185.

[8] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System | Satoshi Nakamoto Institute,” 2008.

[9] M. M. Queiroz, R. Telles, and S. H. Bonilla, “Blockchain and supply chain management

integration: a systematic review of the literature," *Supply Chain Management*, vol. 25, no. 2. Emerald Group Publishing Ltd., pp. 241–254, Aug. 22, 2019, doi: 10.1108/SCM-03-2018-0143.

[10] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*. 2016, doi: 10.1109/ACCESS.2016.2566339.

[11] M. L. Marsal-Llacuna, "Future living framework: Is blockchain the next enabling network?," *Technol. Forecast. Soc. Change*, 2018, doi: 10.1016/j.techfore.2017.12.005.

[12] D. Conte de Leon, A. Q. Stalick, A. A. Jillepalli, M. A. Haney, and F. T. Sheldon, "Blockchain: properties and misconceptions," *Asia Pacific J. Innov. Entrep.*, 2017, doi: 10.1108/apjie-12-2017-034.

[13] W. Al-Saqaf and N. Seidler, "Blockchain technology for social impact: opportunities and challenges ahead," *J. Cyber Policy*, 2017, doi: 10.1080/23738871.2017.1400084.

[14] B. Scott, J. Loonam, and V. Kumar, "Exploring the rise of blockchain technology: Towards distributed collaborative organizations," *Strateg. Chang.*, 2017, doi: 10.1002/jsc.2142.

[15] R. J. Adams, P. Smart, and A. S. Huff, "Shades of Grey: Guidelines for Working with the Grey Literature in Systematic Reviews for Management and Organizational Studies," *Int. J. Manag. Rev.*, 2017, doi: 10.1111/ijmr.12102.

[16] Y. Cai and D. Zhu, "Fraud detections for online businesses: a perspective from blockchain technology," *Financ. Innov.*, 2016, doi: 10.1186/s40854-016-0039-4.

[17] D. Grewal, S. Motyka, and M. Levy, "The Evolution and Future of Retailing and Retailing Education," *J. Mark. Educ.*, 2018, doi: 10.1177/0273475318755838.

[18] McKinsey, "Blockchain technology for supply chains — A must or a maybe?," *McKinsey Co. Oper. Extranet*, pp. 1–10, 2017, [Online]. Available: https://operations-extranet.mckinsey.com.

[19] D. Tranfield, D. Denyer, and P. Smart, “Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review,” *British Journal of Management*. 2003, doi: 10.1111/1467-8551.00375.

[20] M. Petticrew and H. Roberts, *Systematic Reviews in the Social Sciences: A Practical Guide*. 2008.

[21] J. F. Burnham, “Scopus database: A review,” *Biomedical Digital Libraries*. 2006, doi: 10.1186/1742-5581-3-1.

[22] B. Fahimnia, C. S. Tang, H. Davarzani, and J. Sarkis, “Quantitative models for managing supply chain risks: A review,” *European Journal of Operational Research*. 2015, doi: 10.1016/j.ejor.2015.04.034.

[23] E. Barsky, “Mendeley,” *Issues Sci. Technol. Librariansh.*, 2010, doi: 10.5596/c2012-008.

[24] C. Rodr and O. Junio, “Guia de uso de mendeley,” *ISSUU April 15 2010*, 2011, doi: 10.3145/epi.2009.jul.14.

[25] I. Mistry, S. Tanwar, S. Tyagi, and N. Kumar, “Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges,” *Mech. Syst. Signal Process.*, vol. 135, Jan. 2020, doi: 10.1016/j.ymssp.2019.106382.

[26] W. Viriyasitavat, L. Da Xu, Z. Bi, and A. Sapsomboon, “Blockchain-based business process management (BPM) framework for service composition in industry 4.0,” *J. Intell. Manuf.*, 2018, doi: 10.1007/s10845-018-1422-y.

[27] S. Seebacher and R. Schüritz, “Blockchain technology as an enabler of service systems: A structured literature review,” in *Lecture Notes in Business Information Processing*, 2017, doi: 10.1007/978-3-319-56925-3_2.

[28] S. Raman, N. Patwa, I. Niranjan, U. Ranjan, K. Moorthy, and A. Mehta, “Impact of big data on supply chain management,” *Int. J. Logist. Res. Appl.*, 2018, doi: 10.1080/13675567.2018.1459523.

[29] A. Kapitonov, I. Berman, S. Lonshakov, and A. Krupenkin, “Blockchain based protocol for economical communication in industry 4.0,” in *Proceedings - 2018 Crypto Valley Conference on Blockchain Technology, CVCBT 2018*, 2018, doi: 10.1109/CVCBT.2018.00010.

[30] A. Kapitonov, S. Lonshakov, A. Krupenkin, and I. Berman, “Blockchain-based protocol of autonomous business activity for multi-agent systems consisting of UAVs,” in *2017 Workshop on Research, Education and Development of Unmanned Aerial Systems, RED-UAS 2017*, 2017, doi: 10.1109/RED-UAS.2017.8101648.

[31] M. Hung, “Leading the IoT,” *J. Telecommun. Electron. Comput. Eng.*, 2017.

[32] M. H. Miraz and M. Ali, “Blockchain enabled enhanced IoT ecosystem security,” in *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, 2018, doi: 10.1007/978-3-319-95450-9_3.

[33] S. H. Shah and I. Yaqoob, “A survey: Internet of Things (IOT) technologies, applications and challenges,” in *2016 4th IEEE International Conference on Smart Energy Grid Engineering, SEGE 2016*, 2016, doi: 10.1109/SEGE.2016.7589556.

[34] E. Ahmed *et al.*, “The role of big data analytics in Internet of Things,” *Comput. Networks*, 2017, doi: 10.1016/j.comnet.2017.06.013.

[35] H. N. Dai, H. Wang, G. Xu, J. Wan, and M. Imran, “Big data analytics for manufacturing internet of things: opportunities, challenges and enabling technologies,” *Enterp. Inf. Syst.*, 2019, doi: 10.1080/17517575.2019.1633689.

[36] R. Agrawal *et al.*, “Continuous security in IoT using blockchain,” in *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings*, 2018, doi: 10.1109/ICASSP.2018.8462513.

[37] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, “On blockchain and its integration with IoT. Challenges and opportunities,” *Futur. Gener. Comput. Syst.*, 2018, doi: 10.1016/j.future.2018.05.046.

[38] H. F. Atlam, A. Alenezi, M. O. Alassafi, and G. B. Wills, “Blockchain with Internet of

Things: Benefits, challenges, and future directions," *Int. J. Intell. Syst. Appl.*, 2018, doi: 10.5815/ijisa.2018.06.05.

[39] A. Boudguiga *et al.*, "Towards better availability and accountability for IoT updates by means of a blockchain," in *Proceedings - 2nd IEEE European Symposium on Security and Privacy Workshops, EuroS and PW 2017*, 2017, doi: 10.1109/EuroSPW.2017.50.

[40] A. Lastovetska, "Blockchain Architecture Basics: Components, Structure, Benefits & Creation," *MLSDev*, pp. 1–21, 2019, [Online]. Available: https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture.

[41] D. Drescher, *Blockchain basics: A non-technical introduction in 25 steps*. 2017.

[42] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics and Informatics*, vol. 36. Elsevier Ltd, pp. 55–81, Mar. 01, 2019, doi: 10.1016/j.tele.2018.11.006.

[43] J. L. Zhao, S. Fan, and J. Yan, "Overview of business innovations and research opportunities in blockchain and introduction to the special issue," *Financial Innovation*. 2016, doi: 10.1186/s40854-016-0049-2.

[44] S. Haber and W. S. Stornetta, "How to time-stamp a digital document," *J. Cryptol.*, 1991, doi: 10.1007/BF00196791.

[45] D. Bayer, S. Haber, and W. S. Stornetta, "Improving the Efficiency and Reliability of Digital Time-Stamping," in *Sequences II*, 1993.

[46] W. Mougayar, "The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology," *John Wiley & Sons*. 2016.

[47] N. Hackius and M. Petersen, "Blockchain in Logistics and Supply Chain: Trick or Treat?," *Reinf. Plast.*, 2017, doi: 10.15480/882.1444.

[48] P. Helo and Y. Hao, "Blockchains in operations and supply chains: A model and

reference implementation," *Comput. Ind. Eng.*, vol. 136, pp. 242–251, Oct. 2019, doi: 10.1016/j.cie.2019.07.023.

[49] I. Önder and H. Treiblmaier, "Blockchain and tourism: Three research propositions," *Ann. Tour. Res.*, 2018, doi: 10.1016/j.annals.2018.03.005.

[50] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K. K. R. Choo, "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?," *IEEE Cloud Comput.*, 2018, doi: 10.1109/MCC.2018.011791712.

[51] M. Risius and K. Spohrer, "A Blockchain Research Framework: What We (don't) Know, Where We Go from Here, and How We Will Get There," *Bus. Inf. Syst. Eng.*, 2017, doi: 10.1007/s12599-017-0506-0.

[52] D. Cosset, "Blockchain: What is mining?," pp. 1–22, 2018, [Online]. Available: https://dev.to/damcosset/blockchain-what-is-mining-2eod.

[53] N. Szabo, "Bit gold," *Unenumerated*, 2005.

[54] N. Reiff, "How does a block chain prevent double-spending of Bitcoins?," *Investopedia*, pp. 1–4, 2020, [Online]. Available: http://www.investopedia.com/ask/answers/061915/how-does-block-chain-prevent-doublespending-bitcoins.asp.

[55] C. S. Wright, "Bitcoin: A Peer-to-Peer Electronic Cash System," *SSRN Electron. J.*, 2019, doi: 10.2139/ssrn.3440802.

[56] G. O. Karame, E. Androulaki, and S. Čapkun, "Double-spending fast payments in Bitcoin," in *Proceedings of the ACM Conference on Computer and Communications Security*, 2012, doi: 10.1145/2382196.2382292.

[57] M. Crosby, Nachiappan, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain Technology - BEYOND BITCOIN," *Berkley Eng.*, 2016, doi: 10.1515/9783110488951.

[58] A. Chakravarty and P. Guy, "The Product Manager ' s guide to the Blockchain — Part 1," pp. 1–18, 2016.

[59] G. Wood, “Ethereum: a secure decentralised generalised transaction ledger,” *Ethereum Proj. Yellow Pap.*, pp. 1–32, 2014, doi: 10.1017/CBO9781107415324.004.

[60] F. Youssef, “Ripple : Overview and Outlook,” pp. 4–10, 2020.

[61] M. Pournader, Y. Shi, S. Seuring, and S. C. L. Koh, “Blockchain applications in supply chains, transport and logistics: a systematic review of the literature,” *Int. J. Prod. Res.*, vol. 58, no. 7, pp. 2063–2081, Apr. 2020, doi: 10.1080/00207543.2019.1650976.

[62] G. Greenspan, “Ending the bitcoin vs blockchain debate,” pp. 1–10, 2015, [Online]. Available: http://www.multichain.com/blog/2015/07/bitcoin-vs-blockchain-debate/.

[63] K. Francisco and D. Swanson, “The Supply Chain Has No Clothes: Technology Adoption of Blockchain for Supply Chain Transparency,” *Logistics*, 2018, doi: 10.3390/logistics2010002.

[64] A. Rosic, “What is Blockchain Technology? A Step-by-Step Guide For Beginners.” 2016, doi: 781107415324.004.

[65] Andrew Tar, “Proof-of-Work, Explained | Cointelegraph,” *Proof-of-Work, Explain.*, vol. 33, pp. 1–6, 2018, [Online]. Available: https://cointelegraph.com/explained/proof-of-work-explained.

[66] C. Hammerschmidt, “Consensus in Blockchain Systems. In Short.,” *Medium.Com*, pp. 1–11, 2017, [Online]. Available: https://medium.com/@chrshmmmr/consensus-in-blockchain-systems-in-short-691fc7d1fefe.

[67] H. Brabbani, “What is Hashing & Digital Signature in The Blockchain?,” *Blockgeeks*, pp. 1–7, 2017, [Online]. Available: https://blockgeeks.com/what-is-hashing-digital-signature-in-the-blockchain/.

[68] A. Rosic, “Learn All About Cryptocurrencies Cryptography : How Does it All Work ?,” pp. 1–52, 2017, [Online]. Available: https://blockgeeks.com/guides/cryptocurrencies-cryptography/.

[69] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*. 2014.

[70] R. R. Oliveira, "Criptografia simétrica e assimétrica: os principais algoritmos de cifragem," *Online Magazine Digital Security - 5th edition and 6th edition*, 2012.

[71] A. Narayanan and J. Clark, "Bitcoin's academic pedigree," *Communications of the ACM*. 2017, doi: 10.1145/3132259.

[72] Pedro Martins, *Introdução à Blockchain*, 1ª Edição. Livraria, 2018.

[73] R. C. Merkle, "A certified digital signature," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 1990, doi: 10.1007/0-387-34805-0_21.

[74] Selkey, "What is a Merkle Tree and How Does it Affect Blockchain Technology? - SelfKey," pp. 1–11, 2019, [Online]. Available: https://selfkey.org/what-is-a-merkle-tree-and-how-does-it-affect-blockchain-technology/.

[75] S. Cheng, B. Zeng, and Y. Z. Huang, "Research on application model of blockchain technology in distributed electricity market," in *IOP Conference Series: Earth and Environmental Science*, 2017, doi: 10.1088/1755-1315/93/1/012065.

[76] J. Al-Jaroodi and N. Mohamed, "Blockchain in Industries: A Survey," *IEEE Access*, vol. 7, pp. 36500–36515, 2019, doi: 10.1109/ACCESS.2019.2903554.

[77] J. Mattila and T. Seppälä, "Blockchains as a Path to a Network of Systems. An Emerging New Trend of the Digital Platforms in Industry and Society," *ETLA Rep.*, 2015.

[78] D. Cosset, "Blockchain: what is in a block?," *Dev.to*, pp. 1–19, 2017, [Online]. Available: https://dev.to/damcosset/blockchain-what-is-in-a-block-48jo.

[79] D. E. V Community, "Explaining blockchain basics What is it in simple words ? Anatomy of a block," pp. 1–9, 2020.

[80] J. Frankenfield, "What Is Nonce?," pp. 1–6, 2019.

[81] T. M. Fernández-Caramés and P. Fraga-Lamas, “A Review on the Use of Blockchain for the Internet of Things,” *IEEE Access*. 2018, doi: 10.1109/ACCESS.2018.2842685.

[82] B. C. Florea, “Blockchain and Internet of Things data provider for smart applications,” in *2018 7th Mediterranean Conference on Embedded Computing, MECO 2018 - Including ECYPS 2018, Proceedings*, 2018, doi: 10.1109/MECO.2018.8406041.

[83] A. Kiayias, E. Koutsoupias, M. Kyropoulou, and Y. Tselekounis, “Blockchain mining games,” in *EC 2016 - Proceedings of the 2016 ACM Conference on Economics and Computation*, 2016, doi: 10.1145/2940716.2940773.

[84] H. Gjermundrød, K. Chalkias, and I. Dionysiou, “Going beyond the coinbase transaction fee: Alternative reward schemes for miners in blockchain systems,” in *ACM International Conference Proceeding Series*, 2016, doi: 10.1145/3003733.3003773.

[85] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, “A review on consensus algorithm of blockchain,” in *2017 IEEE International Conference on Systems, Man, and Cybernetics, SMC 2017*, 2017, doi: 10.1109/SMC.2017.8123011.

[86] A. M. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. 2016.

[87] M. Pilkington, “Blockchain technology: Principles and applications,” in *Research Handbooks on Digital Transformations*, 2016.

[88] C. Dannen, *Introducing Ethereum and Solidity*. 2017.

[89] M. Castro and B. Liskov, “Practical Byzantine Fault Tolerance and Proactive Recovery,” *ACM Trans. Comput. Syst.*, 2002, doi: 10.1145/571637.571640.

[90] Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, “Blockchain challenges and opportunities: A survey,” *Int. J. Web Grid Serv.*, 2018, doi: 10.1504/IJWGS.2018.095647.

[91] P. Yeoh, “Regulatory issues in blockchain technology,” *J. Financ. Regul. Compliance*, 2017, doi: 10.1108/JFRC-08-2016-0068.

[92] G. W. Peters and E. Panayi, “Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money,” *New Econ. Wind.*, 2016, doi: 10.1007/978-3-319-42448-4_13.

[93] H. Wu, Z. Li, B. King, Z. Ben Miled, J. Wassick, and J. Tazelaar, “A distributed ledger for supply chain physical distribution visibility,” *Inf.*, 2017, doi: 10.3390/info8040137.

[94] T. Swanson, “Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems,” 2015. doi: 10.1017/CBO9781107415324.004.

[95] V. Babich and G. Hilary, “What Operations Management Researchers Should Know About Blockchain Technology,” *SSRN Electron. J.*, 2018, doi: 10.2139/ssrn.3131250.

[96] B. Academy, “What Is a Blockchain Consensus Algorithm?,” *Binance Acad.*, pp. 1–18, 2020, [Online]. Available: https://www.binance.vision/blockchain/what-is-a-blockchain-consensus-algorithm%0Ahttp://files/160/what-is-a-blockchain-consensus-algorithm.html.

[97] M. B. Same, “Blockchain Consensus Encyclopedia Infographic,” pp. 1–2, 2020.

[98] C. Walter, “Categorizing consensus,” 2018. https://tokens-economy.gitbook.io/consensus/categorizing-consensus (accessed May 12, 2020).

[99] C. Walter, “Blockchain Consensus,” *Encyclopedia of Big Data Technologies*, 2019. https://tokens-economy.gitbook.io/consensus/blockchain-consensus (accessed May 12, 2020).

[100] A. Back, “Hashcash - A Denial of Service Counter-Measure,” *Http://Www.Hashcash.Org/Papers/Hashcash.Pdf*, 2002.

[101] B. C. Encyclopedia, “Proof of Work ( PoW ),” 2020. https://tokens-economy.gitbook.io/consensus/chain-based-proof-of-work/proof-of-work-pow-1.

[102] V. Saini, “ConsensusPedia: An Encyclopedia of 30+ Consensus Algorithms - By,” pp. 1–62, 2018, [Online]. Available: https://hackernoon.com/consensuspedia-an-encyclopedia-of-29-consensus-algorithms-e9c4b4b7d08f.

[103] I. Bentov, A. Gabizon, and A. Mizrahi, “Cryptocurrencies without proof of work,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2016, doi: 10.1007/978-3-662-53357-4_10.

[104] D. Kronovet and GitHub, “Proof of Stake,” *GitHub Ethereum Wiki*, 2017. .

[105] L. Lamport, R. Shostak, and M. Pease, “The Byzantine Generals Problem,” *ACM Trans. Program. Lang. Syst.*, 1982, doi: 10.1145/357172.357176.

[106] M. Castro and B. Liskov, “Practical Byzantine Fault Tolerance,” *Proc. Symp. Oper. Syst. Des. Implement.*, 1999, doi: 10.1145/571637.571640.

[107] K. Concepts *et al.*, “Hyperledger Fabric Model Chaincode,” pp. 1–4, 2018.

[108] D. Mazieres and D. Mazières, “The stellar consensus protocol: A federated model for internet-level consensus,” *Stellar Dev. Found.*, 2015.

[109] NEO, “NEO Smart Economy,” *Www.Neo.Org*, 2014. .

[110] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, “Proof of Activity,” *ACM SIGMETRICS Perform. Eval. Rev.*, 2014, doi: 10.1145/2695533.2695545.

[111] Investopedia, “Proof of Activity (Cryptocurrency),” pp. 10–11, 2019, [Online]. Available: https://www.investopedia.com/terms/p/proof-activity-cryptocurrency.asp.

[112] P4Titan, “Slimcoin: A Peer-to-Peer Crypto-Currency with Proof-of-Burn,” *Whitepaper*, 2014.

[113] K. Karantias, A. Kiayias, and D. Zindros, “Proof-of-Burn,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2020, doi: 10.1007/978-3-030-51280-4_28.

[114] Investopedia, “Proof of Burn ( PoB ),” pp. 1–3, 2020.

[115] Investopedia, “Proof of Capacity – Burstcoin,” pp. 2–4, 2020.

[116] S. Gauld, F. Von Ancoina, and R. Stadler, “The Burst Dymaxion An Arbitrary Scalable, Energy Efficient and Anonymous Transaction Network Based on Colored Tangles,” *CryptoGuru PoC SIG*, 2017.

[117] S. Park, A. Kwon, G. Fuchsbauer, P. Gaži, J. Alwen, and K. Pietrzak, “SpaceMint: A Cryptocurrency Based on Proofs of Space,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2018, doi: 10.1007/978-3-662-58387-6_26.

[118] A. Miller, A. Juels, E. Shi, B. Parno, and J. Katz, “Permacoin: Repurposing bitcoin work for data preservation,” in *Proceedings - IEEE Symposium on Security and Privacy*, 2014, doi: 10.1109/SP.2014.37.

[119] investopedia, “Proof of Elapsed Time (Cryptocurrency),” pp. 10–11, 2018, [Online]. Available: https://www.investopedia.com/terms/p/proof-elapsed-time-cryptocurrency.asp.

[120] L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, and W. Shi, “On security analysis of proof-of-elapsed-time (PoET),” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2017, doi: 10.1007/978-3-319-69084-1_19.

[121] Hyperledger sawtooth, “Hyperledger Sawtooth,” *Https://Sawtooth.Hyperledger.Org*. 2019.

[122] A. Saad and S. Y. Park, “Decentralized directed acyclic graph based DLT network,” in *ACM International Conference Proceeding Series*, 2019, doi: 10.1145/3312614.3312647.

[123] Investopedia, “Direct Acyclic Graph Tangle ( DAG ),” pp. 10–11, 2020.

[124] S. Popov, “IOTA whitepaper v1.4.3,” *New Yorker*, 2018.

[125] H. Pervez, M. Muneeb, M. U. Irfan, and I. Ul Haq, “A Comparative Analysis of DAG-Based Blockchain Architectures,” in *ICOSST 2018 - 2018 International Conference on Open Source Systems and Technologies, Proceedings*, 2019, doi: 10.1109/ICOSST.2018.8632193.

[126] M. Swan, *Blockchain: Blueprint for a new economy*. 2015.

[127] Everledger, “Everledger | Tech for Good Blockchain Solutions,” 2020. https://www.everledger.io (accessed May 13, 2020).

[128] C. Gutierrez and A. Khizhniak, “A Close Look at Everledger—How Blockchain Secures Luxury Goods | Altoros,” *Altoros*, 2017. .

[129] Hyperledger, “Advancing business blockchain adoption through global open source collaboration,” 2020. https://www.hyperledger.org (accessed May 13, 2020).

[130] I. C. Lin and T. C. Liao, “A survey of blockchain security issues and challenges,” *Int. J. Netw. Secur.*, 2017, doi: 10.6633/IJNS.201709.19(5).01.

[131] K. Wust and A. Gervais, “Do you need a blockchain?,” in *Proceedings - 2018 Crypto Valley Conference on Blockchain Technology, CVCBT 2018*, 2018, doi: 10.1109/CVCBT.2018.00011.

[132] Ethereum, “Ethereum is a global, open-source platform for decentralized applications,” *Ethereum.org*, 2019. https://ethereum.org (accessed May 13, 2020).

[133] D. Efanov and P. Roschin, “The all-pervasiveness of the blockchain technology,” in *Procedia Computer Science*, 2018, doi: 10.1016/j.procs.2018.01.019.

[134] G. Wood, “Ethereum: a secure decentralised generalised transaction ledger,” *Ethereum Proj. Yellow Pap.*, 2014, doi: 10.1017/CBO9781107415324.004.

[135] V. Shermin, “Disrupting governance with blockchains and smart contracts,” *Strateg. Chang.*, 2017, doi: 10.1002/jsc.2150.

[136] Y. Zhang and J. Wen, “The IoT electric business model: Using blockchain technology for the internet of things,” *Peer-to-Peer Netw. Appl.*, 2017, doi: 10.1007/s12083-016-

0456-1.

[137] L. Luu, D. H. Chu, H. Olickel, P. Saxena, and A. Hobor, “Making smart contracts smarter,” in *Proceedings of the ACM Conference on Computer and Communications Security*, 2016, doi: 10.1145/2976749.2978309.

[138] N. Szabo, “Smart Contracts: Building Blocks for Digital Free Markets,” *Extropy J. Transhuman Thought*, 1996, doi: 10.1200/JCO.2011.40.6546.

[139] N. Szabo, “Formalizing and securing relationships on public networks,” *First Monday*, 1997, doi: 10.5210/fm.v2i9.548.

[140] IBM and M. Gupta, *Blockchain for Dummies*, 2nd ed. John Wiley & Sons, Inc., 2018.

[141] H. Anwar, “Smart Contracts : The Ultimate Guide for the Beginners,” 2018. https://101blockchains.com/smart-contracts/ (accessed May 13, 2020).

[142] I. Weber, X. Xu, R. Riveret, G. Governatori, A. Ponomarev, and J. Mendling, “Untrusted business process monitoring and execution using blockchain,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2016, doi: 10.1007/978-3-319-45348-4_19.

[143] V. Buterin, “Ethereum White Paper,” *Etherum*, 2014.

[144] R. Hull, “Blockchain: Distributed event-based processing in a data-centric world,” in *DEBS 2017 - Proceedings of the 11th ACM International Conference on Distributed Event-Based Systems*, 2017, doi: 10.1145/3093742.3097982.

[145] J. WANG, P. WU, X. WANG, and W. SHOU, “The outlook of blockchain technology for construction engineering management,” *Front. Eng. Manag.*, 2017, doi: 10.15302/j-fem-2017006.

[146] B. Düdder and O. Ross, “Timber tracking: Reducing complexity of due diligence by using blockchain technology (position paper),” in *CEUR Workshop Proceedings*, 2017.

[147] J. D. Caytas, “Developing Blockchain Real-Time Clearing and Settlement in the EU,

U.S., and Globally," *Columbia J. Eur. Law*, 2016.

[148] P. De Filippi, "The interplay between decentralization and privacy: the case of blockchain technologies," *J. Peer Prod.*, 2016.

[149] S. Underwood, "Blockchain beyond bitcoin," *Commun. ACM*, 2016, doi: 10.1145/2994581.

[150] J. Hou, H. Wang, and P. Liu, "Applying the blockchain technology to promote the development of distributed photovoltaic in China," *International Journal of Energy Research*. 2018, doi: 10.1002/er.3984.

[151] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling Localized Peer-to-Peer Electricity Trading among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains," *IEEE Trans. Ind. Informatics*, 2017, doi: 10.1109/TII.2017.2709784.

[152] E. Mengelkamp, J. Gärttner, K. Rock, S. Kessler, L. Orsini, and C. Weinhardt, "Designing microgrid energy markets: A case study: The Brooklyn Microgrid," *Appl. Energy*, 2018, doi: 10.1016/j.apenergy.2017.06.054.

[153] E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer, and C. Weinhardt, "A blockchain-based smart grid: towards sustainable local energy markets," in *Computer Science - Research and Development*, 2018, doi: 10.1007/s00450-017-0360-9.

[154] C. Pop, T. Cioara, M. Antal, I. Anghel, I. Salomie, and M. Bertoncini, "Blockchain based decentralized management of demand response programs in smart energy grids," *Sensors (Switzerland)*, 2018, doi: 10.3390/s18010162.

[155] J. J. Sikorski, J. Haughton, and M. Kraft, "Blockchain technology in the chemical industry: Machine-to-machine electricity market," *Appl. Energy*, 2017, doi: 10.1016/j.apenergy.2017.03.039.

[156] M. Haferkorn and J. M. Q. Diaz, "Seasonality and interconnectivity within cryptocurrencies - An analysis on the basis of bitcoin, litecoin and namecoin," in *Lecture Notes in Business Information Processing*, 2015, doi: 10.1007/978-3-319-

28151-3_8.

[157] R3, “The R3 Story,” *About R3*, 2018. .

[158] P. Treleaven, R. G. Brown, and D. Yang, “Blockchain Technology in Finance,” *Computer (Long. Beach. Calif).*, 2017, doi: 10.1109/MC.2017.3571047.

[159] D. Schwartz, N. Youngs, and A. Britto, “The Ripple protocol consensus algorithm,” *Ripple Labs Inc White Pap.*, 2014.

[160] W. Reijers, F. O’Brolcháin, and P. Haynes, “Governance in Blockchain Technologies & Social Contract Theories,” *Ledger*, 2016, doi: 10.5195/ledger.2016.62.

[161] H. Hou, “The application of blockchain technology in E-government in China,” in *2017 26th International Conference on Computer Communications and Networks, ICCCN 2017*, 2017, doi: 10.1109/ICCCN.2017.8038519.

[162] M. Mettler, “Blockchain technology in healthcare: The revolution starts here,” in *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services, Healthcom 2016*, 2016, doi: 10.1109/HealthCom.2016.7749510.

[163] K. Peterson, R. Deeduvanu, P. Kanjamala, and K. Boles, “A Blockchain-Based Approach to Health Information Exchange Networks,” *Proc. NIST Work. Blockchain Healthc.*, 2016.

[164] T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, and B. Amaba, “Blockchain technology innovations,” in *2017 IEEE Technology and Engineering Management Society Conference, TEMSCON 2017*, 2017, doi: 10.1109/TEMSCON.2017.7998367.

[165] A. Juneja and M. Marefat, “Leveraging blockchain for retraining deep learning architecture in patient-specific arrhythmia classification,” in *2018 IEEE EMBS International Conference on Biomedical and Health Informatics, BHI 2018*, 2018, doi: 10.1109/BHI.2018.8333451.

[166] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, “The Blockchain as a Decentralized Security Framework [Future Directions],” *IEEE Consum. Electron.*

*Mag.*, 2018, doi: 10.1109/MCE.2017.2776459.

[167] N. Kshetri, “Blockchain’s roles in strengthening cybersecurity and protecting privacy,” *Telecomm. Policy*, 2017, doi: 10.1016/j.telpol.2017.09.003.

[168] L. R. Cohen, L. Samuelson, and H. Katz, “How securitization can benefit from blockchain technology,” *J. Struct. Financ.*, 2017, doi: 10.3905/jsf.2017.23.2.051.

[169] N. Bozic, G. Pujolle, and S. Secci, “A tutorial on blockchain and applications to secure network control-planes,” in *2016 3rd Smart Cloud Networks and Systems, SCNS 2016*, 2017, doi: 10.1109/SCNS.2016.7870552.

[170] D. Tapscott and A. Tapscott, “How blockchain will change organizations,” *MIT Sloan Manag. Rev.*, 2017, doi: 10.7551/mitpress/11645.003.0010.

[171] A. Bogner, M. Chanson, and A. Meeuw, “A decentralised sharing app running a smart contract on the ethereum blockchain,” in *ACM International Conference Proceeding Series*, 2016, doi: 10.1145/2991561.2998465.

[172] W. Ying, S. Jia, and W. Du, “Digital enablement of blockchain: Evidence from HNA group,” *Int. J. Inf. Manage.*, 2018, doi: 10.1016/j.ijinfomgt.2017.10.004.

[173] R. Bdiwi, C. De Runz, S. Faiz, and A. A. Cherif, “Towards a New Ubiquitous Learning Environment Based on Blockchain Technology,” in *Proceedings - IEEE 17th International Conference on Advanced Learning Technologies, ICALT 2017*, 2017, doi: 10.1109/ICALT.2017.37.

[174] M. Sharples and J. Domingue, “The blockchain and kudos: A distributed system for educational record, reputation and reward,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2016, doi: 10.1007/978-3-319-45153-4_48.

[175] M. Turkanović, M. Hölbl, K. Košič, M. Heričko, and A. Kamišalić, “EduCTX: A blockchain-based higher education credit platform,” *IEEE Access*, 2018, doi: 10.1109/ACCESS.2018.2789929.

[176] P. Devine, “Blockchain learning: can crypto-currency methods be appropriated to enhance online learning?,” *ALT Online Winter Conf.*, 2015.

[177] N. Kshetri, “Can Blockchain Strengthen the Internet of Things?,” *IT Prof.*, 2017, doi: 10.1109/MITP.2017.3051335.

[178] N. Kshetri, “1 Blockchain’s roles in meeting key supply chain management objectives,” in *International Journal of Information Management*, 2018, doi: 10.1016/j.ijinfomgt.2017.12.005.

[179] D. E. O’Leary, “Configuring blockchain architectures for transaction information in blockchain consortiums: The case of accounting and supply chain systems,” *Intell. Syst. Accounting, Financ. Manag.*, 2017, doi: 10.1002/isaf.1417.

[180] IBM Institute for Business Value, “Forward Together: Three ways blockchain Explorers chart a new direction,” 2017.

[181] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, “Blockchain for IoT security and privacy: The case study of a smart home,” in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2017*, 2017, doi: 10.1109/PERCOMW.2017.7917634.

[182] R. Polim, Q. Hu, and S. Kumara, “Blockchain in megacity logistics,” in *67th Annual Conference and Expo of the Institute of Industrial Engineers 2017*, 2017.

[183] S. Apte and N. Petrovsky, “Will blockchain technology revolutionize excipient supply chain management?,” *Journal of Excipients and Food Chemicals*. 2016.

[184] A. Banerjee, “Integrating Blockchain with ERP for a Transparent Supply Chain,” *Infosys*, 2017.

[185] Y. Madhwal and P. B. Panfilov, “Blockchain and supply chain management: Aircrafts’ parts’ business case,” in *Annals of DAAAM and Proceedings of the International DAAAM Symposium*, 2017, doi: 10.2507/28th.daaam.proceedings.146.

[186] P. R. Newswire, “SYNCFAB Announces Utility Token Sale on Blockchain for Supply

Chain Management and Smart Manufacturing," *SyncFab-token-sale*. 2017.

[187] L. Pawczuk, R. Massey, and D. Schatsky, "Breaking blockchain open Deloitte's 2018 global blockchain survey," 2018. doi: 10.1002/ejoc.201200111.

[188] J. Hinckeldeyn and J. Kreutzfeldt, "Blockchain in der Logistik – Ein Vergleich prototypischer Anwendungen," in *Logistik im Wandel der Zeit – Von der Produktionssteuerung zu vernetzten Supply Chains*, 2019.

[189] Z. C. Kennedy *et al.*, "Enhanced anti-counterfeiting measures for additive manufacturing: Coupling lanthanide nanomaterial chemical signatures with blockchain technology," *J. Mater. Chem. C*, 2017, doi: 10.1039/c7tc03348f.

[190] J. H. Lee and M. Pilkington, "How the Blockchain Revolution Will Reshape the Consumer Electronics Industry [Future Directions]," *IEEE Consum. Electron. Mag.*, 2017, doi: 10.1109/MCE.2017.2684916.

[191] A. W. K. Tan, Y. F. Zhao, and T. Halliday, "A blockchain model for less container load operations in China," *Int. J. Inf. Syst. Supply Chain Manag.*, 2018, doi: 10.4018/IJISSCM.2018040103.

[192] K. Toyoda, P. Takis Mathiopoulos, I. Sasase, and T. Ohtsuki, "A Novel Blockchain-Based Product Ownership Management System (POMS) for Anti-Counterfeits in the Post Supply Chain," *IEEE Access*, 2017, doi: 10.1109/ACCESS.2017.2720760.

[193] H. Subramanian, "Decentralized Blockchain-based electronic marketplaces," *Commun. ACM*, 2018, doi: 10.1145/3158333.

[194] J. W. Forrester, "Industrial Dynamics: A Major Breakthrough for Decision Makers," in *The Roots of Logistics*, 2012.

[195] S. Min, Z. G. Zacharia, and C. D. Smith, "Defining Supply Chain Management: In the Past, Present, and Future," in *Journal of Business Logistics*, Mar. 2019, vol. 40, no. 1, pp. 44–55, doi: 10.1111/jbl.12201.

[196] A. Richardson, "Using Customer Journey Maps to Improve Customer Experience,"

*Harvard Business Review*. 2010.

[197] B. Dickinson, “Blockchain has the potential to revolutionize the supply chain,” *TechCrunch*, 2016.

[198] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, “Blockchain technology and its relationships to sustainable supply chain management,” *Int. J. Prod. Res.*, 2019, doi: 10.1080/00207543.2018.1533261.

[199] V. Babich and G. Hilary, “Distributed ledgers and operations: What operations management researchers should know about blockchain technology,” *Manuf. Serv. Oper. Manag.*, 2020, doi: 10.1287/MSOM.2018.0752.

[200] L. Kehoe, N. O’Connell, D. Andrzejewski, K. Gindner, and D. Dalal, “When two chains combine: Supply chain meets blockchain,” *Deloitte*, 2017.

[201] P. Brody, “How blockchain is revolutionizing supply chain management,” 2017.

[202] M. Dobrovnik, D. Herold, E. Fürst, and S. Kummer, “Blockchain for and in Logistics: What to Adopt and Where to Start,” *Logistics*, 2018, doi: 10.3390/logistics2030018.

[203] Techracers, “How is Blockchain Disrupting the Fintech Industry? - Techracers - Medium,” *Medium*, 2018. https://hackernoon.com/how-is-blockchain-disrupting-the-supply-chain-industry-f3a1c599daef.

[204] W. (Derek) Du, S. L. Pan, D. E. Leidner, and W. Ying, “Affordances, experimentation and actualization of FinTech: A blockchain implementation study,” *J. Strateg. Inf. Syst.*, 2019, doi: 10.1016/j.jsis.2018.10.002.

[205] S. Aggarwal and N. Kumar, “Hyperledger,” *Adv. Comput.*, 2020, doi: 10.1016/bs.adcom.2020.08.016.

[206] Hyperledger, “Hyperledger Fabric,” vol. 46, pp. 1–14, 2020, doi: 10.16383/j.aas.c190516.

[207] E. Androulaki *et al.*, “Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains,” in *Proceedings of the 13th EuroSys Conference, EuroSys*

*2018*, 2018, doi: 10.1145/3190508.3190538.

[208] H. Sawtooth, “Distinctive Features of Sawtooth Separation Between the Application Level and the Core System,” pp. 1–9, 2020.

[209] Ethereum, “The foundation for our digital Ethereum is future,” pp. 1–6, 2020.

[210] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, and V. Santamaría, “Blockchain and smart contracts for insurance: Is the technology mature enough?,” *Futur. Internet*, 2018, doi: 10.3390/fi10020020.

[211] S. E. Fawcett, P. Osterhaus, G. M. Magnan, J. C. Brau, and M. W. McCarter, “Information sharing and supply chain performance: The role of connectivity and willingness,” *Supply Chain Manag.*, 2007, doi: 10.1108/13598540710776935.

[212] J. Kembro, K. Selviaridis, and D. Näslund, “Theoretical perspectives on information sharing in supply chains: A systematic literature review and conceptual framework,” *Supply Chain Manag.*, 2014, doi: 10.1108/SCM-12-2013-0460.

[213] R. Browne, “There were more than 26,000 new blockchain projects last year - only 8% are still active,” *Cnbc*, pp. 1–6, 2017, [Online]. Available: https://www.cnbc.com/2017/11/09/just-8-percent-of-open-source-blockchain-projects-are-still-active.html.

[214] ESI Engineering Specialties Inc, “How Are Safety-Critical Automotive Parts Manufactured ?,” pp. 1–8, 2020.

[215] N. Navet and F. Simonot-Lion, *Automotive embedded systems handbook*. 2017.