A IMPORTÂNCIA DO USO DE BLOCKCHAIN ENQUANTO SOLUÇÃO TECNOLÓGICA NUM MUNDO DE TRANSFORMAÇÃO DIGITAL

Hélder Azeredo[1], Ricardo Passos[2]

[1]*Instituto Superior de Contabilidade e Administração do Porto (Portugal)*
[2]*Instituto Superior de Contabilidade e Administração do (Portugal)*

Resumo

Com este artigo pretendemos aferir a importância do uso de *Blockchain* enquanto solução tecnológica para maior segurança, em uma era onde a transformação digital está presente em todos os negócios. Deste modo iremos apresentar informação que nos irá elucidar quando ao nível de segurança e eficiência da *Blockchain*.

Palavras-chave: *Blockchain*, segurança, transformação digital.

1 INTRODUÇÃO

Temos por hipótese de trabalho que a segurança não entra na equação aquando da elaboração da estratégia de transformação digital em todas as empresas. Deste modo, pretendemos aferir a importância do uso de *Blockchain,* enquanto solução tecnológica disruptiva, para caminhar lado a lado com a transformação digital, que deve acompanhar qualquer negócio. Para tanto, iremos apresentar a concepção de transformação digital

1.1 Transformação Digital

A sociedade está em constante mudança, sendo as novas tecnologias as principais responsáveis. Assim, podemos afirmar que atualmente vivemos em um mundo de informação em tempo real, era digital ou sociedade da informação, conforme Werthein (2000).

A Era digital, sobretudo graças à Internet, revolucionou as nossas vidas. Alterou a forma como obtemos a informação, comunicamos e interagimos com as outras pessoas e organizações. Estas ganharam maior visibilidade, mas, ao mesmo tempo, ampliou-se a concorrência. No entanto, para que os benefícios desta Era alcancem a todos é preciso ter em conta a preocupação externada pelo diretor geral da *Intel Security* no Brasil, que refere que é

> "preciso pensar na segurança como parte fundamental de um negócio e com ela acompanhar a transformação digital e não a considerar apenas como um projeto na área de TI. A segurança é na verdade um habilitador do modelo de negócios, e é preciso ter noção da totalidade de riscos aos quais o negócio está exposto e criar um processo mais integrado e seguro." (Kanamaru, 2019)

Acrescenta ainda que é preciso inovação, mas "a segurança da informação precisa ser incluída no processo desde o início e evoluir como parte fundamental do negócio." (Kanamaru, 2019)

Com as tendências tecnológicas que vivenciamos hoje em dia como por exemplo a *big data*, internet das coisas, mobilidade, *cloud computing*, no futuro, irão obrigar a grandes mudanças no seio corporativo e todas as empresas incorporarão no seu modelo de negócio a tecnologia ou serão empresas de tecnológicas.

1.1.1 Solução tecnológica disruptiva

Segundo Diniz (2017) com a *Blockchain* emerge uma nova tecnologia disruptiva.

Em Outubro de 2008, foi publicado em um grupo de discussão sobre a criptografia o artigo Bitcoin: a *peer-to-peer electronic cash system*, assinado por Satoshi Nakamoto. Esse artigo propunha "uma versão de dinheiro eletrónico que permite pagamentos on-line enviados diretamente de pessoa a pessoa sem passar por uma instituição financeira".

De facto, a crise financeira mundial 2007-2008 foi a oportunidade para o *blockchain* se transformar em um sucesso e daí tem surgido várias aplicações potenciais, tais como na área das finanças, governamental, produtiva, distribuição de mídias, gestão de identidade, transferência de ativos, rastreamento logístico.

1.2 Blockchain

A *Blockchain* é uma tecnologia que regista eventos (ex: transações financeiras) num banco de dados distribuído entre múltiplos dispositivos conectados, designados por nodo ou nós, numa rede descentralizada com uma estampa de tempo e com uma assinatura digital.

A descentralização da *Blockchain*, ou seja, a repartição dos dados em blocos por diferentes membros tem como objetivo simultâneo garantir a segurança e a confiança da rede.

Diniz (2017) explica que "pelo *Blockchain*, a rede inteira mantém o registro atualizado das transações efetivadas em seus domínios, auditável para todos os que dela participam". A *Blockchain* funciona assim como um livro de registos.

1.2.1 Como funciona a Blockchain?

De acordo com a IBM(«Blockchain basics», 2018), a *Blockchain* ao invés de confiar numa terceira parte, como por exemplo uma instituição financeira para mediar transações, os nós, membros de uma rede *Blockchain,* utilizam um protocolo, designado de consenso para coincidir com o conteúdo contábil, *hashes* criptográficos e assinaturas digitais e, desta forma, garantir a integridade das transações.

O protocolo de consenso garante que os livros compartilhados sejam cópias exatas reduzindo o risco de transações fraudulentas, porque a sua adulteração teria que ocorrer em muitos lugares exatamente ao mesmo tempo.

Os *hashes* criptográficos, como o algoritmo computacional SHA256, garantem que qualquer alteração na entrada de transação - mesmo a alteração mais minúscula - resulte em um valor de *hash* diferente, a ser calculado, o que indica entrada de transação potencialmente comprometida.

As assinaturas digitais garantem que as transações sejam originadas de remetentes (assinados com chaves privadas) e não de impostores.

É importante referir que a *Blockchain* é composta por três partes principais, a seguir designadas:

Bloco - é uma lista de transações registadas em um determinado período de tempo com base no tamanho, período e evento desencadeador para o bloco, sendo este diferente para cada *Blockchain*. Para melhor compreensão do que significa bloquear em uma cadeia, podemos usar a metáfora um livro, que é uma cadeia de páginas.

Chain - um *hash*, calculado em tempo real, que liga um bloco a outro, como páginas de livros. Esta parte do encadeamento é difícil de compreender. Funciona como a cola mágica para manter os *Blockchain*s juntos. O *hash* é conhecido como a impressão digital dos dados e bloqueia os blocos em ordem e hora. O algoritmo de *hash* seguro (SHA) é usado para gerar funções *hash* em *Blockchain*. O SHA-256 é um algoritmo comum usado para gerar um *hash* quase exclusivo de 256 bits (32 bytes) de tamanho fixo. Cada *Blockchain* conterá *hash* para garantir a integridade da cadeia.

Rede - composta de nós completos, onde cada nó contém um registo completo de todas as transações que foram registadas naquele *Blockchain*.

Na ilustração abaixo é apresentado um esquema que permite facilmente perceber como funciona o *Blockchain* (Diniz, 2017):

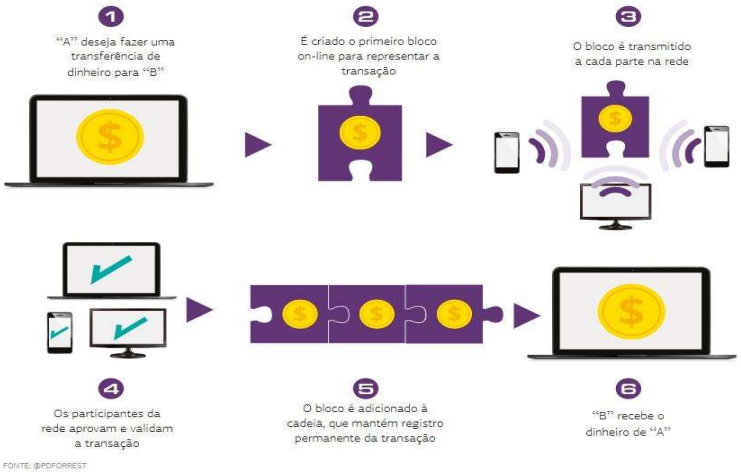

Figura 1 - Como funciona a Blockchain (Fonte: @PDFORREST – (Diniz,2017))

1.2.2 Blockchain é segura?

Com a aplicação cada vez mais extensa da *Blockchain* e com o desenvolvimento de cada vez mais aplicações que usam esta tecnologia, na mesma medida tem vindo a crescer a preocupação, com a segurança dos dados.

Atualmente, os invasores usam as características do próprio *Blockchain* para realizar vários ataques aos dados do *Blockchain*.

Zhu et al., (2018), investigaram as vulnerabilidades da *Blockchain* e realizaram uma classificação abrangente e um resumo da segurança dos dados de *Blockchain*, conforme apresentado na figura abaixo.

Table 1: Classification of Blockchain Attacks

Data privacy attacks			
Transaction privacy attacks	Identity privacy attacks		
[10, 21, 22]	[10, 21, 22, 23, 24, 27, 28]		
Data availability attacks			
Network traceability attacks	Eclipse attacks		
[31, 32, 33, 11, 12]	[34, 35, 12, 36, 37, 38, 39]		
Data integrity attacks			
Double-spending attacks	Selfish mining attacks	Block withholding attacks	
[40, 41, 25, 37, 43, 44]	[15, 45, 46, 47, 48]	[17, 15, 45, 49, 50]	
Data controllability attacks			
Logic problems	Semantic misunderstandings	Design problems verifier's dilemma	Privacy preservation
[51]	[16]	[52]	[53, 54]

Figura 2 - Classificação dos Ataques na Blockchain (Fontr: Zhu et.al,(2018))

Da classificação e posterior investigação estes autores concluíram que os ataques de privacidade de dados apresentam vazamento de dados ou dados obtidos por invasores por meio de análise. Os ataques de disponibilidade de dados apresentam acesso anormal ou incorreto a dados de *Blockchain*. Os ataques de integridade de dados apresentam dados *Blockchain* sendo adulterados. E os ataques de controlabilidade de dados apresentam dados *Blockchain* acidentalmente manipulados por vulnerabilidade de contrato inteligente.

1.2.3 Uma solução para melhorar a eficiência e segurança da Blockchain no Ecommerce

Com a transformação digital que está em curso, ainda mais com a tecnologia disruptiva que traz a *Blockchain*, verifica-se um maior numero de ataques informáticos como se pode constatar com na investigação de Zhu et al., (2018).

Assim importa encontrar soluções que garantam a segurança, mas também a eficiência para permitir que a transformação digital que vivenciamos seja positiva para toda a sociedade.

Segundo Xie et al., (2018) melhorar a eficiência e o desempenho é um tópico importante no mundo de hoje. Como é bem conhecido, a computação cooperativa é uma abordagem tradicional e eficaz e é amplamente utilizada em vários campos. No caso do comércio eletrónico, a tecnologia de segurança tornou-se uma questão importante, restringindo o rápido desenvolvimento e a popularização do comércio eletrónico.

As soluções existentes aproveitam os protocolos *Blockchain* para melhorar a credibilidade das transações, mas a maioria delas têm algumas limitações, como menor taxa de transferência e maior latência de consenso. Esses problemas tornam a tecnologia *Blockchain* difícil de ser amplamente usada.

Xie et al., (2018) apresentam um *framework* confiável "*Trusted Trading Framework Based on Blockchain in Ecommerce*"(ETTF) usando o protocolo *Blockchain* no e-commerce para alcançar uma negociação com maior credibilidade. O ETTF inclui um protocolo *Blockchain* de pares *"peer*

blockchain protocol" (PBP) baseado em uma arquitetura *Blockchain* de pares para suportar o armazenamento de transações massivas e transações instantâneas. No PBP, as escalas de taxa de transferência são quase linearmente aumentadas com a computação: quanto mais poder de computação disponível, mais blocos são selecionados por unidade de tempo. Além disso, a fim de garantir uma maior segurança das transações, introduziram um algoritmo de consenso forte (ECA) no comércio eletrónico. O ETTF também é eficiente porque o número de mensagens requeridas é quase linear no tamanho da rede.

Xie et al., (2018) apresentam na figura seguinte uma comparação entre a *Blockchain* derivado de Bitcoin e o ETTF:

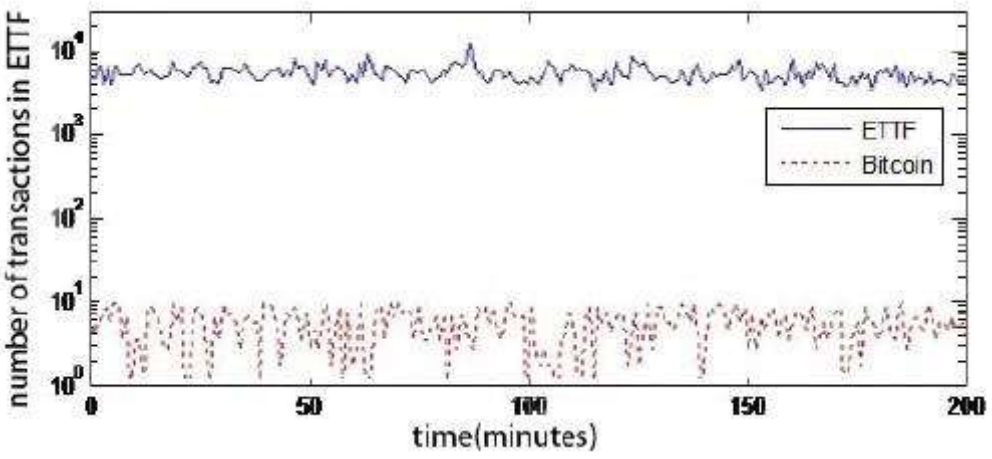

Figura 3: Comparação Bitcoin(Blockchain) e ETTF (Fonte:(Xie et al., 2018))

Facilmente podemos constatar que o ETTF mostra melhor desempenho na taxa de transferência, latência e capacidade no e-commerce quando comparado com a *Blockchain* derivado de Bitcoin.

2 METODOLOGIA

Para alcançar o objetivo pretendido neste artigo, foi feita uma revisão bibliográfica de alguns artigos científicos da área, comparando resultados, pretendendo absorver o máximo de informação e obter a opinião de especialistas com diferentes realidades científicas e empresariais, para assim fazer uma análise crítica do uso da *Blockchain* no e-commerce

3 RESULTADOS

Na revisão de literatura efetuada, apresentamos o que se entende por transformação digital, o que se compreende por *blockchain*, bem como o seu funcionamento e de que forma o *Blockchain* é uma solução disruptiva na transformação digital que atualmente presenciamos.

Por fim apresentamos uma solução para melhorar a eficiência e segurança da *Blockchain* no Ecommerce.

4 CONCLUSÕES

As tecnologias *Blockchain* representam uma maneira fundamentalmente nova de fazer negócios. Elas criaram uma próxima geração robusta e inteligente de aplicativos para registo e troca de ativos físicos, virtuais, tangíveis e intangíveis. Graças aos conceitos-chave de segurança criptográfica, consenso descentralizado e um livro público compartilhado (com sua visibilidade

devidamente controlada e autorizada), as tecnologias *Blockchain* podem mudar profundamente a forma como organizamos as nossas atividades económicas, sociais, políticas e científicas.

A própria *Blockchain* procura revolucionar os setores tradicionais, e assim sendo caminhar ao lado da transformação digital nos diferentes tipos de negócios. No entanto, uma nova tecnologia baseada na *Blockchain* já provou ter uma melhor eficiência, mostrando melhor desempenho em algumas áreas. Essa tecnologia ETTF, mostra melhor desempenho na taxa de transferência, latência e capacidade no e-commerce.

Desta forma é possível concluir que a *Blockchain* é uma tecnologia muito importante para acompanhar o processo de transformação digital dos mais diversos negócios, enquanto tecnologia eficiente, no entanto é importante não descartar outras tecnologias e perceber quais se aplicam mais ao nosso negócio.

É importante reiterar que a segurança é um fator muito importante e que deve fazer parte fulcral no plano de transformação digital de um negócio, no entanto, dependendo do tipo de negócio e transformação, deve ser feita uma análise, no sentido de saber qual a tecnologia mais eficiente e que se adapte melhor ao nosso negócio.

REFERÊNCIAS

Blockchain basics: Introduction to distributed ledgers. (2018, Março 18). Obtido 24 de Março de 2019, de IBM Developer website: https://developer.ibm.com/tutorials/cl-blockchain-basics-intro-bluemixtrs/

Diniz, E. H. (2017). Emerge uma nova tecnologia disruptiva. GV-executivo, 16(2), 46. https://doi.org/10.12660/gvexec.v16n2.2017.68676

Kanamaru, M. (2019). O papel da segurança da informação na transformação digital. Obtido 6 de Abril de 2019, de http://www.tibahia.com/tecnologia_informacao/conteudo_unico.aspx?c=ART_TECH&fb=B_FUL L&hb=B_CENTRA&bl=LAT1&r=ART_TECH&nid=39024

Werthein, J. (2000). A sociedade da informação e seus desafios. Ciência da Informação, 29(2), 71–77. https://doi.org/10.1590/S0100-19652000000200009

Xie, W., Zhou, W., Kong, L., Zhang, X., Min, X., Xiao, Z., & Li, Q. (2018). ETTF: A Trusted Trading Framework Using Blockchain in E-commerce. 2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design ((CSCWD)), 612–617. https://doi.org/10.1109/CSCWD.2018.8465233

Zhu, L., Zheng, B., Shen, M., Yu, S., Gao, F., Li, H., … Gai, K. (2018). Research on the Security of Blockchain Data: A Survey. ArXiv:1812.02009 [Cs]. Obtido de http://arxiv.org/abs/1812.02009