Blockchain Technologies

André Martins, Ana Teresa Gomes, and Pedro Barbosa

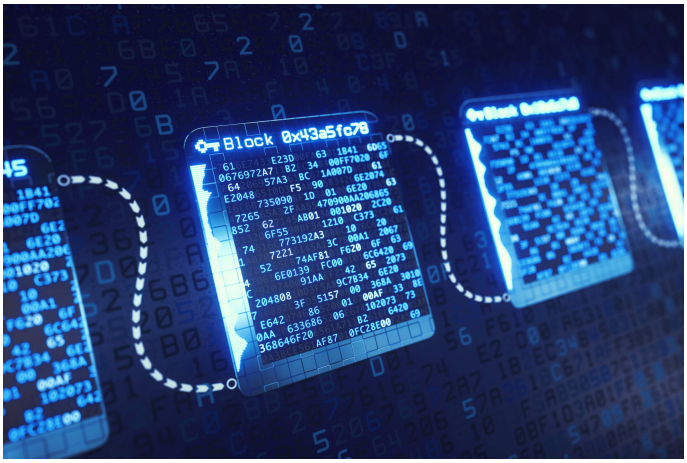
University of Minho, Department of Informatics, 4710-057 Braga, Portugal
e-mail: {a89586,a89536,a89529}@alunos.uminho.pt

Abstract. Este trabalho tem como principal objetivo aprofundar os conhecimentos sobre blockchain. Blockchain é uma tecnologia que surgiu em 2008 e que funciona através do método de cadeia de blocos, blocos estes que são estruturas digitais onde é inserido um conjunto de transações. Esta tecnologia ficou mundialmente conhecida pois é a base estrutural de uma criptomoeda chamada Bitcoin. Assim, através deste ensaio escrito, pretendemos conhecer melhor o que é blockchain, como surgiu e como funciona, quais as suas principais vantagens e desvantagens e quais as suas aplicações no mundo atual. Então o que é blockchain?

1 BLOCKCHAIN TECHNOLOGIES

Ao revolucionar a forma como a informação é transmitida, as tecnologias de blockchain apresentam-se como algo revolucionário. Sendo uma tecnologia descentralizada, imutável, extremamente transparente que mantém, ao mesmo tempo, a segurança dos seus utilizadores, esta tecnologia promete inovar o nosso mundo, desde a mais simples transação até aos mais complexos sistemas bancários.

Neste ensaio escrito, iremos dar uma breve explicação sobre o que é o blockchain e os diferentes usos que pode ter no nosso quotidiano.



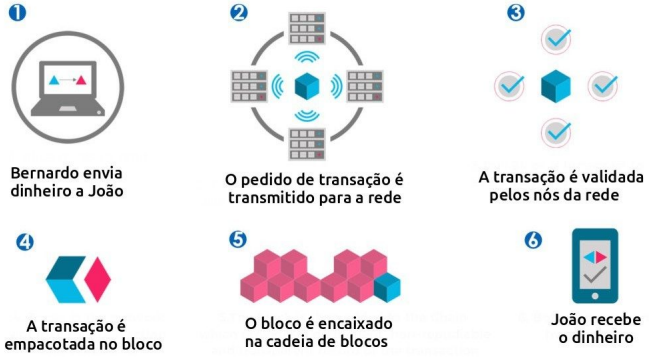
2 O que é Blockchain?

De uma forma geral, esta é uma inovadora tecnologia que torna possível transferências de variadíssimas informações de um emissor A para um destinatário B, tendo como base três princípios-chave: descentralização, transparência e imutabilidade. Deste modo, todos os registos de transações são públicos mas com utilizadores encriptados, transmitindo confiança e abertura entre remetente e destinatário e, consequentemente, torna mais fácil a sua comunicação.

Apesar de ainda estar numa fase muito embrionária do seu desenvolvimento, esta tecnologia é bastante promissora. Se fizermos um paralelo com o protocolo TCP/IP, sobre o

qual assenta a Internet e o modo de vida moderno, vemos que também demorou vários anos até o seu uso ser massivo e global. Podemos perspetivar o mesmo para a tecnologia blockchain, estando esta no início da sua caminhada até ao uso global, tornando-se num dos pilares em que se irão assentar as tecnologias das próximas décadas.

Uma das maiores revoluções que esta tecnologia poderá realizar é a diminuição drástica do custo de transações financeiras, visto que passaram a funcionar num modelo "peer-to-peer" e deixaria de ser necessária a intervenção direta de um intermediário. Se, no futuro, este sistema for adotado globalmente, irá, certamente, provocar uma reforma profunda nos sistemas bancários e financeiros de todo o mundo.



3 Como surgiu e como funciona?

Esta tecnologia é associada ao surgimento da Bitcoin, em 2008. Como é explicado no documento de apresentação da Bitcoin, Bitcoin: A Peer-to-Peer Electronic Cash System, e explicado pelo autor deste documento, Satoshi Nakamoto, a Blockchain é descrita como “A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through institution." [6].

Mas como funciona, realmente, a blockchain? Como é que permite transações entre 2 entidades sem a necessidade de haver um intermediário? Poderá esta nova tecnologia revolucionário sistemas bancários e financeiros?

Como também é referido neste artigo, as semelhanças entre o surgimento da tecnologia blockchain e do protocolo TCP/IP são claras. Como o e-mail permitiu uma troca de mensagens direta entre um sujeito A e um sujeito B, a Bitcoin permite uma transação bilateral entre A e B, sem a necessidade de um intermediário. O surgimento do TCP/IP também baixou, significativamente, o custo das comunicações, assim como a blockchain promete baixar drasticamente o custo das transações financeiras. Pode, potencialmente, ser o sistema primário e global de todas as transações financeiras. Se tal acontecer, as economias globais sofrerão uma radical mudança, demorada, mas que pode bem ser a realidade das próximas gerações.

Vamos explicar o funcionamento em 5 passos, como são explicados no artigo "The Truth About Blockchain" de Marco Iansiti e Karim R. Lakhani, lançado em 2017 [8].

3.1 1 - Distribued Database

Cada bloco da blockchain tem acesso a toda a base de dados e ao seu histórico. Contudo, nenhum bloco controla a informação nem a base de dados. Cada bloco consegue também ver todas as transações feitas, sem a necessidade de um intermediário.

3.2 2 - Peer to Peer Transmition

A comunicação e as transições realizam-se diretamente entre duas partes, ao invés de existir uma entidade central a mediar as comunicações. Cada bloco guarda e transmite informação para todos os outros blocos.

3.3 3 - Transparency with pseudonymity

Cada transação, bem como o seu montante, são visíveis a todos os blocos da blockchain, tornando-se públicas e transparentes. No entanto, cada bloco é encriptado, possuindo um identificador com 30+ carateres. Os utilizadores podem decidir se querem manter o anonimato ou provar a sua identidade aos restantes utilizadores.

3.4 4 - Irreversibility of records

Uma vez que uma transação é realizada, e os blocos são atualizados, os registos são imutáveis, isto porque eles estão ligados a todas as transações previamente realizadas. Este processo é gerido por vários algoritmos que asseguram a imutabilidade da blockchain, tornando a base de dados permanente, organizada cronologicamente, e visível para todos os outros blocos.

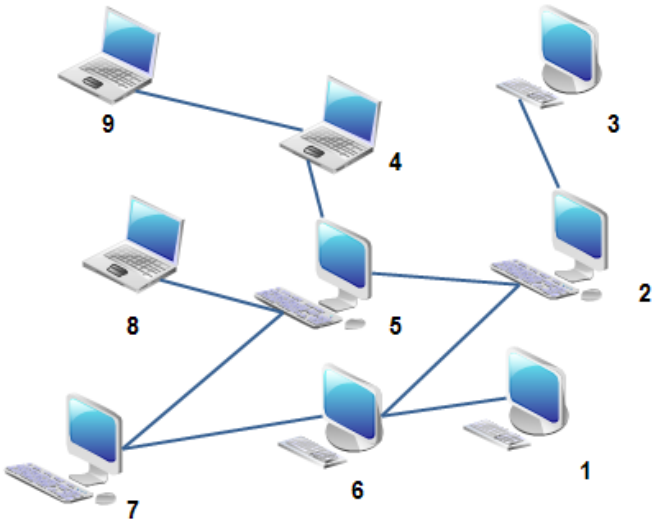
3.5 5 - Computational logic

A natureza digital da blockchain permite que as transações possam ser programadas. Assim sendo, os utilizadores podem criar algoritmos que ativem automaticamente transações entre blocos.

4 Os 3 pilares do Blockchain

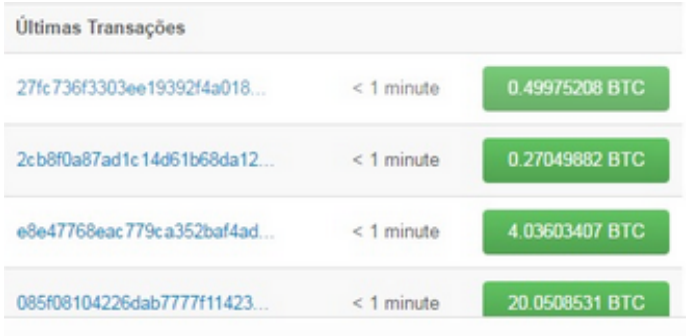
4.1 1 - Descentralização

Ao longo dos últimos anos, sempre foi mais usual os serviços centralizados, ou seja, há a necessidade de interação com esse serviço superior pois caso contrário não existe forma de obter as informações pretendidas. Assim, uma tecnologia como o blockchain, que é descentralizada, tem como base uma rede ponto-a-ponto (esquematizada na imagem abaixo) sem uma entidade superior que possua o controlo absoluto da informação.



4.2 2 - Transparência

Um facto bastante interessante desta nova tecnologia é a capacidade de manter a privacidade dos seus utilizadores, sendo totalmente pública e global. Dois aspetos bastante opostos mas que em blockchain é possível. Isto acontece devido a todas as transações que são feitas pelos utilizadores serem expostas para que qualquer um possa ter acesso. No entanto, cada pessoa está "escondida" por detrás de um código encriptado, que permite a esta manter a sua privacidade ainda que estejam expostos os seus registos de transações.



4.3 3 - Imutabilidade

Esta particularidade de blockchain consiste na impossibilidade de adulteração de dados guardados na rede, que se torna uma das principais vantagens desta tecnologia. Desta forma, ninguém consegue corromper as contas de uma determinada empresa ou indivíduo.

Tudo isto é possível através da função hash criptográfica, ou seja, qualquer input de comprimento variado tem uma saída de comprimento definido. Esta tecnologia consiste numa lista ligada com dados contidos em cada bloco e um ponteiro hash a fazer a ligação entre eles apontando sempre para o bloco anterior. Desta forma, se alguma pessoa tenta alterar os dados de um bloco nº 3, por mais pequena que seja a alteração, o hash irá tornar-se completamente diferente. Se por coincidência o ponteiro hash apontar para o bloco anterior, também o bloco nº 2 irá sofrer alterações e assim sucessivamente. Como podemos ver, uma pequena alteração num dos blocos resultaria numa cadeia de blocos de dados completamente alterada, o que é impossível, provando assim a imutabilidade.

5 Vantagens

5.1 Transações comerciais facilitadas

Devido à redução das interações humanas, há uma menor probabilidade de erro nas transações ou lacunas de informação, tornando assim a comunicação entre as duas partes interessadas muito mais fácil e eficiente.

5.2 Rastreamento dos produtos transacionados

Uma das grandes vantagens da blockchain consiste na possibilidade de confirmar a qualidade e segurança dos produtos, de modo a que nenhuma das partes fique defraudada ou lesada. O elevado grau de transparência que a blockchain nos oferece, permite que todos os utilizadores tenham total conhecimento das transações que estão a ocorrer e do histórico de transações.

5.3 Velocidade nas transações

Já estamos acostumados a, nos dias de hoje, haver algumas instituições que demoram dias a efetuar uma transação, estando até mesmo indesponível aos fins de semana, já para não falar das transações internacionais em que também o fuso horário interfere. Com blockchain isso

não acontece, visto que as transações são imediatas, podem ser efetuadas a qualquer hora do dia e em qualquer dia, incluindo fins de semana, e, até mesmo as internacionais, são efetuadas com elevada rapidez. Ao ser concluída a transação, o utilizador tem acesso a uma confirmação de envio.

6 Desvantagens

Infelizmente, ainda existem algumas desvantagens que fazem com que esta nova tecnologia ainda tenha aspetos para corrigir e evoluir, o que é normal, dado o estado prematuro de desenvolvimento em que ainda se encontra.

6.1 Ataque a 51% da blockchain

Ao ser um sistema puramente digital, é impossível desassociar a possibilidade de uma ataque informático. Para uma entidade tomar controlo de uma rede blockchain, terá que controlar 51% dessa mesma rede. Apesar do algoritmo Proof of Work que protege a Blockchain da Bitcoin, por exemplo, se mostrar bastante seguro, ainda existe da possiblidade de esta sofrer uma ataque. Contudo, e como iremos referir mais à frente quando abordarmos a aplicação da Bitcoin, quanto mais blocos pertencerem a esta rede, mais segura ela se torna, reduzindo bastante a possibilidade de qualquer ataque informático. E, no caso de haver um ataque, este apenas conseguira alterar as transações mais recentes e por um curto período de tempo, uma vez que os blocos estão protegidos criptograficamente, o que tornaria impossível a alteração de blocos mais antigos, com o atual poder computacional que temos ao nosso dispor.

6.2 Chaves privadas

Cada usuário da blockchain, possui uma chave pública e uma chave privada. A primeira pode ser partilhada com outros, no entanto, a segunda diz respeito apenas ao usuário de cada conta e deve ser mantida em sigilo. Se por acaso a pessoa responsável pela conta se esquecer da chave privada, perde todos os seus fundos e não os pode recuperar, representado, assim, enormes perdas financeiras, e não só, que estariam associadas

6.3 Armazenamento

Para além de esta nova tecnologia exigir uma grande capacidade de processamento e uma rede que consiga suportar grandes volumes de dados, atualmente a blockchain do bitcoin necessita de pelo menos 200GB de armazenamento, sendo que, com o seu crescimento, possivelmente irá precisar de cada vez mais.

7 Aplicações do Blockchain

7.1 Toyota

"A Toyota e a Toyota Financial Services, braço financeiro da companhia, lançaram no ano passado uma organização virtual entre os grupos batizada de Toyota Blockchain Lab, que tem avançado sistematicamente em iniciativas para uso da tecnologia blockchain." [5]

Como podemos ver, este lançamento do grupo Toyota é um exemplo de aplicação da blockchain. Com este lançamento, a Toyota espera melhorar a conexão entre pessoas ou empresas devido à grande transparência desta tecnologia (e consequente confiabilidade) e promete ajudar a investir na segurança e proteção de dados. Esta nova tecnologia permite uma transferência de direitos mais fácil, que se tornará num benefício para negócios como venda de carros usados ou serviços de assinatura, devido ao facto de dados pessoais serem partilhados com segurança e à criação de "connected cities". Assim, a blockchain irá ser responsável por novas oportunidades na indústria automobilista e por uma enorme mudança na relação entre o carro e o cliente.

7.2 Bitcoin

Sendo esta a criptomoeda mais famosa e mais valiosa do mercado (1 Bitcoin equivalia a cerca de 10056 euros, no dia 20 de Outubro pelas 14:11), e tendo no seu cerne uma tecnologia blockchain, esta será a aplicação desta tecnologia mais famosa do momento. Voltando a 2008, e ao surgimento da Bitcoin, esta criptomoeda é apresentada por Satoshi Nakamoto, no documento oficial e original "Bitcoin: A Peer-to-Peer Electronic Cash System", deste modo:

"A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending.We propose a solution to the double-spending problem using a peer-to-peer network." [6]

A Bitcoin assenta-se em todos os pilares inerentes a uma blockchain e, neste documento, são explicados, e sustentados com equações matemáticas, depois traduzidas em código, a segurança deste sistema. Para se ter uma ideia, sendo p a probabilidade de um bloco fiável encontrar o próximo bloco, q a probabilidade de um bloco malicioso encontrar o próximo bloco, e Qz a probabilidade um bloco malicioso chegar a outro bloco, estando z blocos atrás.

Através de cálculos matemáticos, para q = 0.3 e z = 20, a probabilidade do sistema sofrer um ataque é de apenas 0,24%. Se z for igual a 30, essa probabilidade já é de 0,015%.

Outra visão, para obtermos probabilidades de ataque bem sucedido abaixo de 0,1%, para um q = 0,45 (45% de probabilidade do bloco malicioso encontrar o próximo bloco, o que é uma probabilidade ridiculamente alta) ao termos um z = 340, existiria uma probabilidade infimamente baixa do ataque ser bem sucedidos.

Mais do que na teoria, a Bitcoin apresenta-se como um sistema bastante fiável e seguro.

Todos estes números e cálculos encontram-se disponíveis em "Bitcoin: A Peer-to-Peer Electronic Cash System" by Satoshi Nakamoto (2008) [2]

7.3 Smart Contracts

Os chamados smart contracts baseiam-se num código if-this-then-that (IFTTT), o que os torna autónomos. Numa situação normal, um intermediário certifica-se de que ambas as partes estão de acordo com o contrato. Utilizando Blockchain, não só se exclui a necessidade de um intermediário, como assegura que todos os participantes têm conhecimento dos termos acordados e que estes mesmos são automáticamente aplicados, uma vez conhecidos.

Este tipo de contrato pode ser utilizado em várias situações financeiras, questões de propriedade, angariação de fundos, entre outras.

8 Conclusão

Concluímos, assim, que a tecnologia blockchain ainda tem algumas falhas,como seria de esperar de algo tão recente e que se encontra numa fase ainda inicial do seu desenvolvimento, no entanto, possui vantagens, algumas delas únicas e com um potencial enorme para revolucionar sistemas económicos e financeiros a nível global, que tornam esta tecnologia extremamente inovadora e como potencial próximo pilar da nossa sociedade, tal como o TCP/IP se tornou ao longo dos anos.

As possibilidades são infinitas, e, neste momento, é quase impossível prever como se encontrará esta tecnologia daqui a 10 ou 20 anos. São cada vez mais as entidades e empresas que investem forte neste tipo de tecnologia, sendo cada vez mais comum o seu uso.

Ninguém sabe ao certo como é que a blockchain irá afetar o nosso dia a dia, mas podemos afirmar, convictamente, que esta tecnologia promete dar muito que falar e que a partir do momento em que tenha uso massificado e global, será algo indispensável e que estará o cerne das tecnologias que dependeremos no futuro.

"But given the time horizons, barriers to adoption, and sheer complexity involved in getting to TCP/IP levels of acceptance, executives should think carefully about the risks involved in experimenting with blockchain. Clearly, starting small is a good way to develop the know-how to think bigger. But the level of investment should depend on the context of the company and the industry. Financial services companies are already well down the road to blockchain adoption. Manufacturing is not.

No matter what the context, there's a strong possibility that blockchain will affect your business. The very big question is when." [8]

References

1. Rosic, Amir: What is Blockchain Technology? A Step-by-Step Guide For Beginners
2. Omnitude: What are the advantages of Blockchain? (2019)
3. Alecrim, Emerson: O que é Blockchain: significado e funcionamento (2017)
4. Binance Academy: Blockchain Advantages and Disadvantages (2020)
5. Blockmaster: TOYOTA BLOCKCHAIN LAB ACELERA USO DA TECNOLOGIA POR MEIO DE INICIATIVAS E COLABORAÇÃO EXTERNA (2020)
6. Nakamoto, Satoshi: Bitcoin: A Peer-to-Peer Electronic Cash System (2008)
7. Rosic, Amir: 17 Blockchain Applications That Are Transforming Society
8. Iansiti, Marco e R. Lakhani, Karim: The Truth About Blockchain (2017