BlockChain

Ana Catarina Gil, Ana Margarida Campos, Tânia Rocha A85176

Abstract: Blockchain é uma tecnologia que se tem vindo a desenvolver ao longo dos anos. Esta tecnologia pode ajudar a resolver diferentes tipos de problemas no mundo industrial e financeiro, como confiança, transparência, segurança e confiabilidade do processamento de dados. Neste artigo é apresentada a descrição e os prós e contras da utilização de blockchain.

Keywords: BlockChain, Bitcoin, Estrutura de dados.

1 BlockChain

1.1 O que é

BlockChain é um tipo de Base de Dados Distribuída que guarda registos de transações de maneira permanente e à prova de alterações por terceiros.

Um bloco é uma parte concreta da BlockChain onde são registadas algumas ou todas as transações desde as mais recentes, e uma vez concluído é guardado na mesma como uma base de dados permanente.

Existe um número incontável de blocos que são ligados uns aos outros - como uma cadeia - onde cada bloco contém uma referência para o bloco anterior.

1.2 De onde surgiu

A tecnologia BlockChain começou a ser desenvolvida entre 1998 e 2008 mas foi totalmente renovada em 2008 num artigo académico denominado por “Bitcoin: um sistema financeiro eletrónico peer-to-peer” publicado por uma pessoa ou grupo sob o pseudónimo de Satoshi Nakamoto.

Este conceito foi criado num cenário de crise económica mundial com o termo Bitcoin que, entre outros, tinha como objetivo prevenir o gasto duplo de valores e aumentar a segurança das transições financeiras pela internet.

Num ambiente digital, onde todos os dados podem ser copiados, alterados e trocados, BlockChain foi a solução perfeita para trazer a segurança necessária em falta para serem realizadas as transições até aí inseguras.

Desde então, visto que este método é a base de criptomoedas, muitos bancos, empresas e organizações governamentais têm demostrado o seu interesse em BlockChain.

2 Bitcoin

A bitcoin é uma moeda totalmente virtual e uma das aplicações de blockchain. Ao contrário de muitos outros métodos de pagamentos virtuais, como o Paypal, a emissão da bitcoin não é controlada por um Banco Central, ou por qualquer outro intermediário. Ela é produzida de forma descentralizada por milhares de computadores e de pessoas que utilizam a capacidade das suas máquinas para as criar e registar todas as transações feitas [5].

Existe um limite para a quantidade de bitcoins existente, 21 milhões, e visa-se que este seja atingido em 2140. Esse limite foi estabelecido pelo criador da moeda, um desenvolvedor misterioso chamado Satoshi Nakamoto — que, até hoje, nunca teve a identidade comprovada.

O preço de compra das bitcoins está em constante alteração por isso não é fácil estabelecer um valor exato para o preço de uma unidade, mas em média estas podem rondar nos milhares de euros.

Devido a esta mesma razão, muitas pessoas apostam no negócio de compra e venda de Bitcoins, visto que, em apenas minutos, o valor destas pode subir ou baixar consideravelmente.

Em 2015, o jornal *The Economist* desenvolveu uma das implementações da segunda geração da blockchain, o Ethereum, como uma linguagem de programação que permite aos utilizadores escreverem contratos inteligentes e mais sofisticados.

Desde a sua criação até 2016, foi estimado o montante de mil milhões de dólares de investimento em tecnologias ligada a BlockChain.

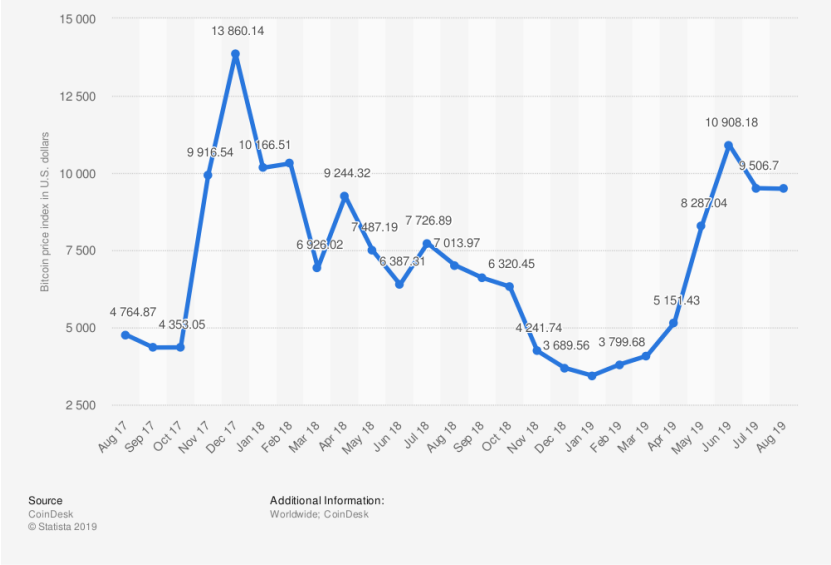

Fig. 1. Indíce do valor da bitcoin de agosto de 2017 até agosto de 2019.

3 Como funciona

Cada bloco contém 3 principais dados: a informação, o hash do bloco e a hash do bloco anterior.

A informação armazenada por um bloco depende do tipo de cadeia de blocos, no caso de blocos associados à Bitcoin, estes guardam os detalhes das transações, ou seja, o remetente, o recetor e a quantidade de moedas (valor da transação).

A hash do bloco é como se fosse uma impressão digital, identifica o bloco assim como todo o seu conteúdo e esta é sempre única. Sempre que um bloco é criado, é calculado a sua hash. Este pode ter diferentes tipos de entrada de dados e consequentemente diferentes tamanhos, no entanto, a saída de dados terá sempre um tamanho fixo.

Deste modo, como a hash criada depende do conteúdo dos blocos, uma mesma entrada resultará sempre na mesma saída, ou seja, não é um método aleatório. No entanto, se for feita uma pequena alteração na entrada, a saída muda completamente.

Outro elemento é a hash do bloco anterior, sendo esta a propriedade que garante a segurança de toda a cadeia.

É possível conseguir aceder a um bloco e alterá-lo, mas como consequência, a sua hash irá alterar-se e invalidar o bloco seguinte, tal como o resto da cadeia. Porém, com a evolução dos computadores, estes conseguem calcular centenas de milhares de hashes por segundo, permitindo assim alterar a informação de um bloco e recalcular todos os hashes para o bloco seguinte.

3.1 “Proof of work”

Para amenizar estes riscos, é usado um mecanismo chamado “Proof-of-work”, que de forma sintetizada, dificulta o processo de cálculo das hashes dos blocos. Este algoritmo é usado principalmente em criptomoedas. Resumidamente, mineradores da rede vão competir entre si para resolver complexos enigmas computacionais, e uma vez resolvidos, o bloco vai finalmente ser transmitido para a rede e confirmado por outros mineradores.

Deste modo, um ataque com sucesso precisaria de muito poder computacional e muito tempo para a realização dos cálculos, e, portanto, seria ineficiente, uma vez que o custo seria maior que a recompensa.

Posto isso, um dos problemas do Proof of Work é o facto da mineração exigir equipamentos muitos caros que consomem grandes quantidades de energia.

4 Vantagens e Desvantagens

4.1 Vantagens

O desenvolvimento de BlockChain potenciou a utilização deste tipo de estrutura, destacando-se os seguintes pontos:

- Não intermediação: permite que uma base de dados seja compartilhada diretamente sem um administrador. Em vez de ter uma lógica e aplicação central, as transações têm a sua própria validação e autorização para impor as restrições permitindo, portanto, que sejam processadas independentemente.
- Segurança dos utilizadores: os utilizadores têm o controlo total de todas as suas informações criando uma rede mais segura.
- Integridade: existe também mais integridade uma vez que as ações a serem executadas são sempre realizadas estritamente de acordo com o protocolo definido.
- Transparência e imutabilidade: importante destacar que as mudanças na blockchain são visíveis publicamente por todos os intervenientes, possibilitando transparência nas transações, sendo que nenhuma pode ser alterada ou eliminada, permitindo assim imutabilidade.
- Transações mais rápidas e de menor custo: dois intervenientes são capazes de fazer uma troca sem supervisão ou intermediação levando a que as transações sejam efetuadas mais rapidamente e com um menor custo.
- Redução da complexidade: Todas as transações são adicionadas à rede pública, reduzindo a desordem e complicações geradas.

4.2 Desvantagens

Existem também algumas desvantagens associadas a esta estrutura de dados, nomeadamente:

- Modificação de informação: alterar dados ou o código de uma rede Blockchain é normalmente muito complicado e geralmente requer um mecanismo onde uma cadeia de blocos é abandonada e outra é criada.
- Redundância: enquanto que as estruturas de dados centralizadas processam transações uma ou duas vezes, em blockchain os dados devem ser processados independentemente por todos os nodos da rede. Portanto, muito mais trabalho para o mesmo resultado.
- Custo: esta estrutura oferece uma grande economia em preço e tempo, mas os altos custos de capital inicial podem ser um impedimento.
- Armazenamento: a velocidade no crescimento de blockchain parece estar a superar a capacidade dos discos rígidos (HDD) e a rede corre o risco de perder nodos se ficar muito grande.
- Questões de integração: com o uso de blockchain existem mudanças significativas a serem realizadas em sistemas já existentes. De maneira a realizar a troca, as empresas precisam de desenvolver uma estratégia de transição.

5 Aplicações de blockchain

Nos bancos a promessa do blockchain como tecnologia confiável e sem intermediários poderia revolucionar pagamentos, captação de capital, securitizações e empréstimos. Além disso, ferramentas como os contratos inteligentes prometem automatizar muitos processos presentes nos bancos nos dias de hoje, como processamento de pedidos e distribuição de testamentos.

Na saúde, blockchain revoluciona a comunicação entre as instituições, com a disponibilização de dados sobre pacientes numa rede compartilhada que pode impactar positivamente a saúde mundial. Um paciente que começa um tratamento noutro país pode ter todos os seus exames e históricos partilhados de forma digitalmente segura, sem que haja edições ou perdas nas informações. Da mesma forma, a troca de experiência entre os médicos com estudos de doenças mundiais, formas de diagnóstico e tratamentos podem ser descentralizadas, criando um Big Data de saúde global. Via blockchain podem ser partilhadas as doenças mais comuns em determinadas regiões do mundo, os medicamentos mais utilizados, o controlo de stock do material de trabalho necessário para os tratamentos, entre outras informações que são importantes de serem compartilhadas.

6 Conclusão

Concluindo, a tecnologia blockchain é útil e versátil para o nosso mundo uma vez que facilita a maioria dos sistemas nos diferentes setores, permitindo um futuro sem fraude e engano. Porém ainda estão a ser feitas pesquisas de forma a diminuir as desvantagens e a expandir a utilização desta estrutura.

7 Referências

[1] Julija Golosova, Andrejs Romanovs: The Advantages and Disadvantages of the Blockchain Technology. IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (2018)

[2] Puneet Kumar Kaushal,, Dr. Amandeep Bagga,, Dr. Rajeev Sobti; Evolution of Bitcoin and Security Risk in Bitcoin Wallets;

[3] Kehrli, J. (07 de outubro de 2016). BlockChain explained.

8 WebGrafia

https://www.binance.vision/pt/blockchain/positives-and-negatives-of-blockchain

http://graphics.reuters.com/TECHNOLOGY-BLOCKCHAIN/010070P11GN/index.html

https://www.savjee.be/videos/simply-explained/how-does-a-blockchain-work/