Blockchain

André Morais[A83899], Pedro Rodrigues[A84783],Luís Ribeiro[A85954]

Universidade do Minho, Braga, Portugal
Rede de Computadores, Grupo 5 PL2

Abstract. A Blockchain é, basicamente, uma base de dados partilhada onde qualquer pessoa pode ter acesso. Para assegurar que as cópias da base de dados não são alteradas, a *network* faz constantes verificações, daí ser muito difícil de ser modificada posteriormente

Keywords: Blockchain, Bitcoin, Criptomoedas, Tokens, Proof-of-Work, P2P.

1 Introdução

1.1 O que é a Blockchain?

A Blockchain é uma base de dados completamente aberta a qualquer pessoa. Uma vez que os dados são escritos num bloco é muito difícil de alterá-los, ou seja, ficam imutáveis.

Cada bloco da *chain* é constituído por: os seus **dados**, que se refere ao tipo de blockchain; a **hash do próprio bloco** que identifica o bloco e todo o seu conteúdo, tornando-o único e a **hash do bloco anterior**, permitindo assim criar a *chain*.

Enquanto base de dados regista as transações de tokens, sejam eles criptomoedas ou algum sistema de votação. Em vez de ser utilizado uma entidade central para controlar a blockchain, é usada uma P2P network (descentralização da blockchain).

A P2P (Peer-to-peer) é uma arquitetura de redes onde cada um dos pontos ou nodos da rede funciona tanto como cliente como servidor, sem a necessidade de um servidor central. Sempre que há uma nova transação é criado um novo bloco, que é exposto a uma validação. Todos os nodos (computadores que partilham essa cadeia) recebem uma cópia da base de dados automaticamente.

A Bitcoin, juntamente com tantas outras moedas, usa tecnologia de blockchain como suporte de funcionamento.

1.2 Porque é que é tão difícil de alterar uma *chain*?

Quando um cliente conecta na network, recebe uma cópia da blockchain. Quando é adicionado um novo bloco, este tem de ser adicionado em todas as cópias de todos os clientes da network.

Primeiramente, para conseguir alterar qualquer bloco da corrente, é necessário alterar todos os restantes blocos, porque se alterarmos apenas um vamos quebrar a corrente, visto que eles guardam, também, a hash do bloco anterior.

Mesmo assim os computadores têm capacidade para alterar todos os blocos de uma corrente em segundos. Para combater isso, existe um algoritmo "*Proof of Work*".

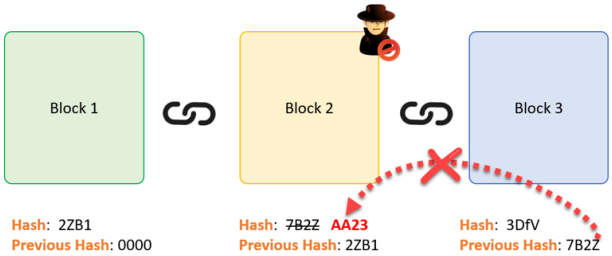

Figure 1 - Tentativa de ataque a um bloco

Smart Contracts (SC)

Smart Contracts (ou SC) são sistemas de computador autónomos, escritos em código, que têm a função de controlar execuções entre indivíduos na blockchain.

Estes contratos são armazenados na blockchain e podem ser usados para a troca automática de moedas baseada em certas condições. Utilizando a linguagem de programação Solidity escrevem-se as regras que se quer ver cumpridas no SC, adicionando esse novo contrato aos outros existentes.

Por serem armazenados em blockchains, estes contratos são imutáveis e distribuídos. Sendo imutáveis, uma vez criados não podem ser mudados. E sendo distribuídos significa que o resultado desse contrato é avaliado por todos na network.

Apesar das regras estarem escritas nos SC, não há nada que os possa supervisionar, surgindo assim o conceito de Mecanismo de Consenso. O **Proof of Work** e o **Proof of Stake** são os mecanismos mais conhecidos, e iremos falar deles em seguida.

"Smart contracts" may be the most transformative blockchain application at the moment. These automate payments and the transfer of currency or other assets as negotiated conditions are met" (Iansiti & Lakhani, 2017).

Proof of Work

O conceito de *Proof of Work* foi desenvolvido para prevenir e reduzir ataques de negação de serviço (DDoS), spams na rede e outros abusos no sistema. Surgiu como tentativa de reduzir os efeitos desses ataques utilizando funções hash.

O PoW é um requisito para definir um cálculo computacional, também chamado de *mining*. Para isso, cada usuário, também conhecido como "miner", é exposto a 2 fases deste processo de *mining*, denominadas de **Verificação** e **Distribuição**.

Esta verificação é realizada através da resolução de um puzzle matemático (descobrir o novo código hash do bloco). Há uma corrida contra o tempo entre os computadores da rede para resolver o problema. A fase de distribuição consiste na entrega de *tokens*/moedas ao primeiro a resolver o dito puzzle.

A competição entre computadores da rede para resolver o mesmo problema resulta num grande consumo de energia.

Como sabemos, o processo de criação de um novo bloco implica o cálculo de um código hash, sendo assim, com o algoritmo de "*Proof of Work*", o cálculo do código hash é muito mais demorado pois implica constantes verificações de modo a que correspondam a determinadas condições. Posto isto, um computador não consegue recalcular os códigos hash de todos os blocos da corrente em segundos, impedindo assim um ataque à corrente.

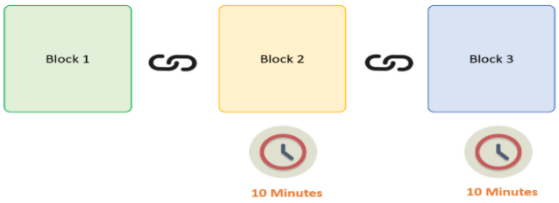

Figure 2- Proof of Work no caso da Bitcoin

Proof Stake

O conceito de *Proof of Stake* surge como alternativa para o *Proof of Work* estudado. Neste mecanismo, em vez de "minors" temos "validadores", e incentiva as pessoas com maior poder monetário a investir na rede.

Para se tornar um validador, cada nodo da *network* tem que depositar dinheiro na rede. Quanto mais dinheiro se deposita, maior a chance de resolver de resolver os puzzles matemáticos. Como prémio, o nodo/usuário recebe as taxas relativas às transações validadas.

Para evitar fraudes, se os nodos aprovarem transações não válidas, irão perder dinheiro depositado na rede. A única maneira de aprovar transações fraudulentas e não ser penalizado por isso é se controlares mais de 50% da rede (51% attack), porém é praticamente impossível.

Apesar da escolha do validador para o novo bloco ser aleatória, quem está a começar ou tem um poder económico inferior está "condenado" à mediocridade.

P2P (Peer-to-Peer) Network

O que é uma Network?

É um grupo de dispositivos interconectados, localmente (cabo) ou sem fios (internet), que trocam informação. O tipo de conexão mais usado é um modelo cliente-servidor centralizado, um único servidor é responsável por todas as tarefas da rede e por guardar toda a informação trocada, ou seja, uma única entidade guarda e controla toda a informação da rede. Isto faz com que seja fácil ter acesso e controlar toda a informação da rede.

A rede utilizada na blockchain é diferente do comum, não há ponto centralizado nem conexão cliente-servidor, em vez disso, toda a informação da rede é constantemente guardada e transferida pelos participantes da mesma. Todos os participantes da rede guardam uma cópia semelhante a toda a informação da rede, estes participantes são conhecidos como "nodos" ou "peer". Então "peer to peer network" é uma rede distribuída que guarda e transfere dados sem um servidor central. Assim, no caso da blockchain, para conseguirmos alterar um bloco, este bloco terá de ser alterado em todos os clientes presentes na rede, fazendo com que seja muito mais complicado atacar a rede e tornando a blockchain mais segura.

"P2P financial market. Blockchain could also help build a P2P financial market in a secure and reliable way. Noyes explored ways of combining peer-to-peer" (Zheng,Z ,Xie,S. ,Dai,H. ,Chen,X. ,Wang,H.,2018).

2 Diferentes tipos de Blockchain

Table 1. Tipos de Blockchain

Propriedade	Public Blockchain	Private Blockchain
Consenso	*Miners*	Uma organização
Permissões de Leitura	Público	Pode ser público ou privado
Imutável	Quase imutável	Pode ser modificado
Eficiência	Baixa	Alta
Centralizada	Não	Sim

3 Porque precisamos da Blockchain?

3.1 Vantagens

Vamos apresentar algumas das vantagens do uso da Blockchain:

Transparência: o facto da blockchain ser pública e visível para a toda a gente, oferece transparência e todas as transações são imutáveis.

Descentralização: As transações armazenadas nos blocos estão contidas em milhões de computadores que participam na cadeia, por isso, é descentralizado, assim, os dados perdidos são sempre recuperáveis.

Segurança: Todas as ferramentas aqui referidas (P2P, Proof of work,…) contribuem para a segurança do Sistema. Todas as transações e dados são anexados ao bloco depois do processo de verificação, existe, assim, um consenso entre todos os participantes sobre o que deve ser registado no bloco.

Fraude: Como existem várias condições de verificações, diminui o risco de fraude.

Redução de tempo e custo: Blockchains não são rápidas, mas são mais baratas e mais rápidas do que transações entre bancos.

Colaboração: Permite fazer transações diretas, não sendo necessário intermediários.

3.2 Desvantagens

A blockchain não é perfeita, e claro que tem as suas desvantagens como por exemplo:

Uso excessivo de energia: A criação de blocos, quando em grandes quantidades concorrentemente, consomem uma grande quantidade de eletricidade. Num mundo onde a crise energética é cada vez mais falada, faz sentido assinalar esta desvantagem da tecnologia.

Ineficiência: Quantas mais transações houver, maior é a informação contida na blockchain. Para fazer ou receber pagamentos tem que se fazer *download* e verificação de toda a *chain*, que pode levar horas e horas.

Mining: Muitos adeptos da blockchain argumentam que os *miners* mantêm a estabilidade e segurança da tecnologia. Isso é verdade apenas se houver *miners* suficientes.
O maior problema é que esses *miners* podem se juntar e conseguirem reescrever ou alterar um registo da blockchain e assim, a segurança dos dados será comprometida.

Private Keys: A blockchain usa criptografia de "public key" para fornecer aos seus users o controlo sobre suas unidades de criptomoeda. Cada endereço da blockchain possui uma chave correspondente. Embora o endereço possa ser compartilhado, a sua chave correspondente é privada, daí ser denominada de "private key". Os users precisam da sua "private key" para aceder aos seus fundos, o que significa que eles agem como seu próprio banco. Se um user perde a sua chave, o dinheiro é efetivamente perdido e não há muito a fazer.

4 Possíveis Usos

A blockchain pode ser usada em diversas formas como podemos observar na seguinte tabela:

Table 2. Usos da Blockchain

Setor	Exemplos
Saúde	○ Desenvolvimento de Contratos Pessoais ○ Gestão de Dados ○ Banco de dados Universal
Artes e Ciências	• Super Computação • P2P recursos • Análises de Multidões
IoT	○ Rede de casas Inteligentes ○ Carros Autónomos ○ Assistentes Digitais ○ Robôs e drones personalizados
Finanças	• Pagamentos • Histórico de transações • Moeda digital (ex.Bitcoin)

5 Conclusão

Em suma, a blockchain é uma "cadeia de blocos" que armazena informação em cada um dos seus blocos. A segurança da blockchain é assegurada por algortimos como o proof-of-work e pela sua descentralização. A noção de P2P network vem desta descentralização, ou seja, não há relação cliente-servidor. Em vez disso, existem vários users (nodos) na network, permitindo assim que a validação dos blocos seja feita por estes, e não por um servidor central. Proof-of-work é um algortimo em que todos os nodos da network "resolvem" um puzzle criptográfico, para saber quem vai "criar" o próximo bloco. Apesar da vantagem da segurança, existem grandes desvantagens como o uso excessivo de energia, devido à criação concorrente de blocos, e a possibilidade da existência de *Minning Pools*.

Concluído o trabalho, entendemos que apresentamos uma pesquisa abrangente sobre a blockchain. Inicialmente, mostramos o que é a blockchain e as suas características. Em seguida, discutimos em que consiste a sua segurança, e analisamos cada um dos seus tópicos. Além disso, apontamos as suas vantagens e desvantagens. No entanto, havia espaço para melhorar neste relatório, pois não aprofundamos algumas noções como a criptomoeda e os outros tipos de algoritmos usados para a segurança da blockchain.

Houve certamente uma aprendizagem notória relativamente à blockchain e aos seus tópicos.

“We believe that more blockchain applications will emerge in the near future in areas as diverse as art, tourism and sports.” (Zhegu & Olleros, 2016)

Referências

1. Iansiti,M.,Lakhani,K. (2017,January-February). The Truth About Blockchain. *Harvard Business Review*,R1701J,10
2. Olleros, F. Xavier, Zhegu,M. (2016). Research Handbook on Digital Transformations. Edward Elgar Publishing. Cheltenham, UK & Northampton,MA,USA
3. Zheng,Z ,Xie,S. ,Dai,H. ,Chen,X. ,Wang,H. (2018). Blockchain challenges and opportunities: a survey. Int. J. Web and Grid Services, Vol. 14, No. 4, 2018
4. https://www.guru99.com/blockchain-tutorial.html
5. http://graphics.reuters.com/TECHNOLOGY-BLOCKCHAIN/010070P11GN/index.html?fbclid=IwAR2G6Rw2_awfepVH4Y3GAduyu3LOSp-QWb8TWDCRTfzjh9NBe2Y_cbO4f2o