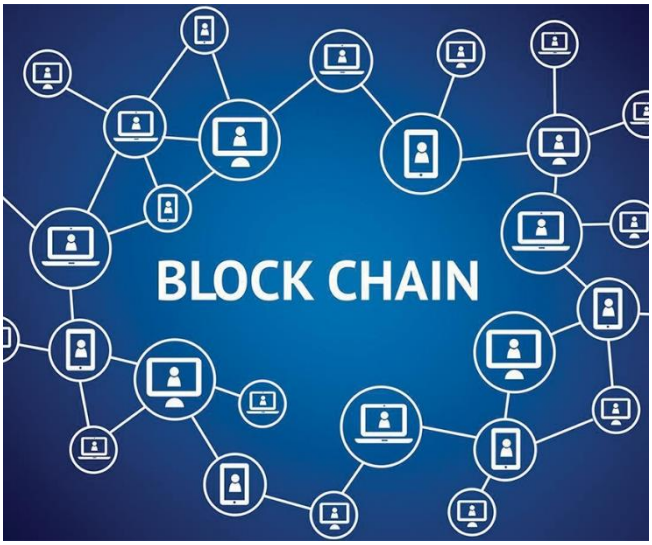
Trabalho Teórica - Blockchain

Grupo 15

Estratégia Organizacional

2020/2021



Trabalho realizado por:

Diogo Dias Lopes– 2018019746;

Leonardo Marques – 2019123778

Ricardo Rodrigues - 2017015954

Índice

Historia da Blockchain

O começo

A ideia por trás da tecnologia blockchain foi descrita no ano de 1991, quando os cientistas da computação Stuart Haber e W. Scott Stornetta introduziram uma solução computacionalmente prática para documentos digitais, uma vez que eles eram gerados com registro de data que não podiam ser adulterados.

O sistema utilizava uma cadeia de blocos protegidos criptograficamente para armazenar os documentos com registo de data e hora. Em 1992 as Merkle trees1 foram incorporadas ao projeto, tornando-o mais eficiente e permitindo que vários documentos fossem coletados em um único bloco. No entanto, esta tecnologia não foi amplamente utilizada e a patente expirou em 2004, quatro anos antes do início do Bitcoin.

Utilização da blockchain na Bitcoin

No final de 2008, um white paper introduzindo um sistema de dinheiro eletrônico peer-to-peer ou (par-a-par) descentralizado chamado Bitcoin foi postado em uma lista de discussão de criptografia por uma pessoa ou grupo usando o pseudônimo de Satoshi Nakamoto.

Com base no algoritmo de Proof of Work Hashcash, mas ao invés de utilizar uma função de computação confiável de hardware como o RPoW, a proteção de gasto duplo em Bitcoin foi fornecida por um protocolo peer-to-peer descentralizado para rastrear e verificar as transações. Em suma, os Bitcoins são "minerados" para gerar uma recompensa se utilizando do Proof of Work por mineiros individuais e depois verificados pelos nós descentralizados na rede.

Em 3 de janeiro de 2009, o Bitcoin ganhou vida quando o primeiro bloco de Bitcoin foi minerado por Satoshi Nakamoto, que foi recompensado com 50 Bitcoins. O primeiro destinatário a receber Bitcoins foi Hal Finney que recebeu 10 Bitcoins de Satoshi Nakamoto na primeira transação de bitcoin do mundo no dia 12 de janeiro de 2009.

Apesar de toda esta evolução, o boom da bitcoin e subsequentemente da blockchain só se deu no final de 2017, com a bitcoin a ultrapassar a fasquia do milhar de dólar e a partir daí começou a ser uma tecnologia *mainstream*.

Na imagem a seguir pode ser verificado esse pico de valor que a bitcoin atingiu no final de 2017:

Figura 1 – Gráfico da variância de valor da bitcoin entre 2017 e 2021

Uso da blockchain em eleições

Em 2018 nas eleições da Virgínia pela primeira vez numas eleições foi dada a opção de voto através de uma app mobile baseada em blockchain. 144 pessoas conseguiram votar através de 31 países. Esta novidade demonstrou-se um sucesso tanto que em 2019 voltou-se a repetir a possibilidade do voto se realizar através de Blockchain.

Blockchain = Cripto moedas/Bitcoin

Com a análise da história da blockchain grande parte da sua história é relacionada com a Bitcoin, apesar disso devemos distinguir os termos. A blockchain é de facto a tecnologia por detrás e que possibilita o uso da Bitcoin e das cripto moedas. Apesar de a blockchain ser usada sobretudo no mercado das cripto moedas esta tecnologia pode e tem sido aplicada em vários outras áreas como vamos poder ver ao decorrer deste relatório. Contudo esta relação entre a blockchain e cripto moedas pode ser considerado um indício para o quanto esta tecnologia é considerada segura e o impacto que a sua utilização pode estabelecer.

Descentralização

Ao analisarmos a história da blockchain podemos verificar que ao início foi introduzida como uma forma diferente para gerir documentos mas realmente onde houve o boom desta tecnologia foi para tentar arranjar uma solução alternativa ao modelo com que as transações eram realizadas(bancos).

Isto é, como até então eram feitas as transações? Se uma pessoa queria passar certo montante para outra esta transação teria que passar por uma entidade considerada de confiança pelos dois para que esse montante fosse transferido.

Na imagem seguinte podemos ver esse mesmo contraposto entre um sistema centralizado e uma representação de uma blockchain.

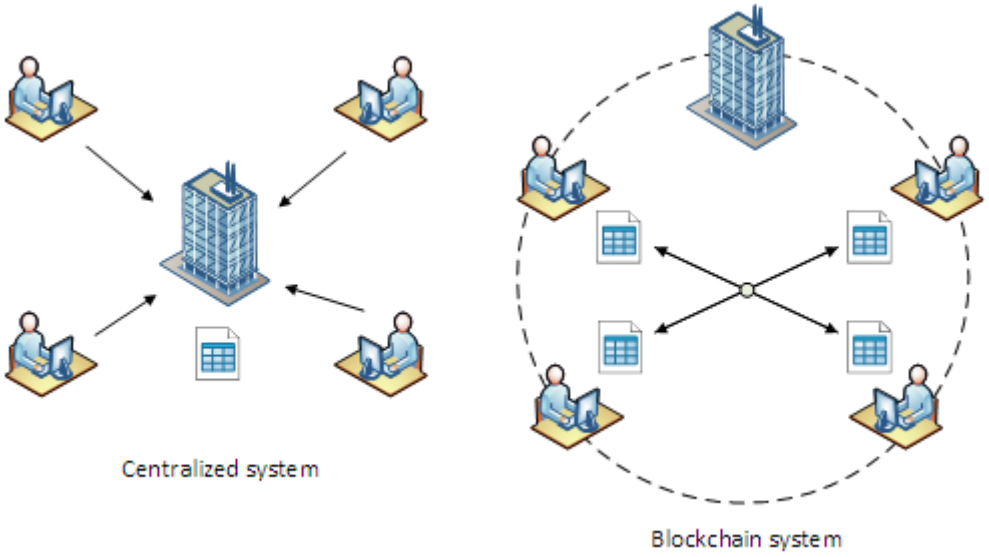


Figura 2 – Sistema centralizado VS Blockchain

Um dos problemas desta solução seria o da real legitimidade dessa mesma entidade intermédia e se esta podia ser substituída ou mesmo inexistente noutro tipo de modelo. Surgiu então a ideia da blockchain. A solução proposta pela blockchain pretende descentralizar o ator que media as transações por milhares de atores que criam uma cadeia e que a seguram a credibilidade destas mesmas transações. Mas o que realmente é a blockchain?

O que é a blockchain?

Blockchain parece complicado, e definitivamente pode ser, mas seu conceito central é realmente muito simples. Um blockchain é um tipo de base de dados. Mas não uma base de dados relacional como já estudamos em anteriores unidades curriculares (Base de dados e Arquitetura e Administração de Base de Dados).
Uma diferença importante entre uma base de dados relacional e um blockchain é a maneira como os dados são estruturados. Uma blockchain guarda informações em grupos, também conhecidos como blocos, que contêm conjuntos de informações. Os blocos têm certas capacidades de armazenamento e, quando preenchidos, são encadeados no bloco previamente preenchido, formando uma cadeia de dados conhecida como "blockchain". Todas as novas informações que seguem aquele bloco recém-adicionado são compiladas em um bloco recém-formado que também será adicionado à cadeia depois de preenchido. Uma base de dados estrutura os seus dados em tabelas, enquanto um blockchain, como seu nome indica, estrutura seus dados em pedaços (blocos) que são encadeados. Este sistema também inerentemente cria uma

linha do tempo irreversível de dados quando implementado de forma descentralizada. Quando um bloco é preenchido, ele é gravado em pedra e se torna uma parte desta linha do tempo. Cada bloco na cadeia recebe um carimbo de data / hora exato quando é adicionado à cadeia.

Estrutura

Como anteriormente foi referido, a blockchain pode ser comparada a um tipo de base de dados mas como é esta estruturada e os conceitos base da sua implementação

A blockchain tem por base dois conceitos fundamentais, ser aberta e distribuída.

A aberta, pois todos os membros da blockchain têm acesso a todas as transações realizadas na mesma e distribuída pois todos os membros compartilham entre si a mesma sequencia de transações.

O bloco

Mas para percebermos estes conceitos vamos falar primeiro na unidade básica desta cadeia(blockchain), o bloco. Um bloco é um espaço de memória em que são normalmente guardados os atributos da transação de informação que ocorreu, estes atributos podem ser por exemplo o valor da transação se esta transação for monetária, a data e a hora e por fim um atributo especial. Este atributo especial é a hash, ou chave, que normalmente é uma sequência, encriptada ou não, aleatória de carateres que permite que um bloco quando é criado e validado pela blockchain seja ligado ao último bloco presente na mesma. Mas como decorre a validação das transações/blocos?

O minerador

Aqui é nos introduzidos uma entidade base para uma blockchain: o minerador.

O minerador é a entidade que certifica se uma transação é válida. Esta fase de validação decorre da seguinte forma.

1ª fase: Validação da transação:

Quando ocorre uma transação o minerador vai verificar se o individuo que transfere o montante/informação detém esse mesmo montante/informação, sendo esta parte a mais fácil. Por exemplo, o José quer transferir 10 euros para o Manuel primeiramente o minerador verifica se o José detém estes 10 euros,

2ª fase: Encontrar a chave hash e publicação da solução

Posteriormente o minerador tenta encontrar a chave hash, correspondente á transação. Após encontrada esta mesma chave o minerador partilha a chave bem como os dados da transação para o resto da blockchain, sendo este bloco adicionado aos restantes membros da cadeia. Esta procura pela chave normalmente é uma competição entre vários mineradores, o que permite a que a transação seja exposta para o restante da cadeia o mais rápido possível. Em norma o minerador demora cerca de 10 minutos a encontrar esta mesma chave.

Estes 10 minutos correspondem a uma utilização computacional e energética considerável e é a fase que mantem a cadeia o mais segura possível. Estes mineradores são normalmente recompensados e incentivados pelo esforço tanto computacional coo energético através de cripto moedas, como é o caso da Bitcoin.

Na figura seguinte é ilustrado os passos de uma transação em blockchain:

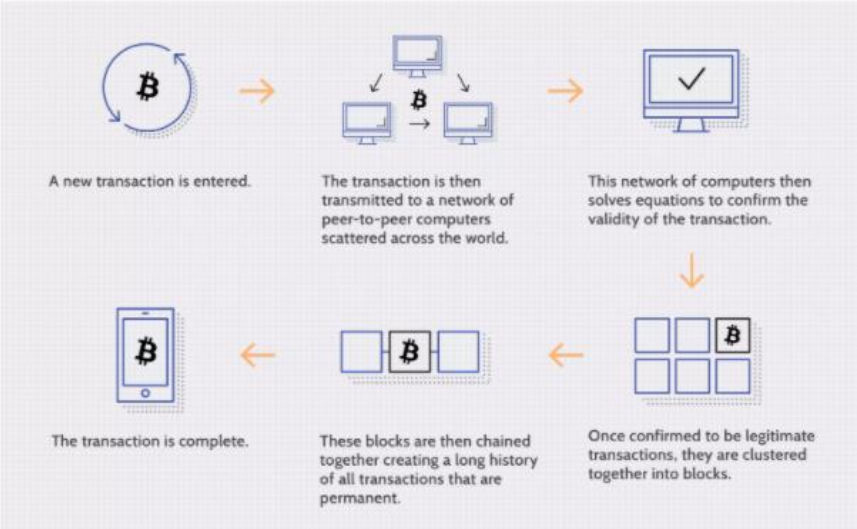


Figura 3 – Passos de uma transação em blockchain

Segurança

A blockchain realmente parece a solução perfeita para esta temática das transações de informação entre indivíduos/entidades. Mas será que esta solução é mesmo perfeita?

Não, a blockchain tal como quase tudo criado pelo homem não é perfeito.

Apesar de ser muito difícil a blockchain ser adulterada, devido ao facto de a alteração de um bloco implicar a alteração de todos os blocos anteriores devido ao facto de as chaves hash ser alterada, esta adulteração e sim possível.

Esta adulteração é possível através do ataque dos 51%. Este ataque baseia-se em um individuo/entidade possuir 51% da blockchain, o que permite que a restante parte(49%-minoria) não se aperceba quando a maioria adultera dados dentro da blockchain. Apesar desta adulteração ser possível esta é muito dispendiosa, tanto em termos computacionais como energéticos. Um estudo de 2019 revelou que seria necessário cerca de 260 mil dólares para fraudar a bitcoin sendo que este valor aumenta sempre que outro bloco se junta á rede, sendo que este número só tende a crescer á medida que a blockchain cresce.

Vantagens e desvantagens

Tal como referido antes, apesar de toda a sua complexidade, o potencial da blockchain como uma forma descentralizada de manutenção de transações é quase ilimitado. A maior privacidade do utilizador, segurança elevada, as taxas de processamento mais baixas e menos erros, a tecnologia blockchain são algumas das vantagens em relação a outras soluções. Apesar disso esta também tem algumas desvantagens.

Na tabela a seguir estão inumeradas algumas vantagens e desvantagens da mesma:

Vantagens	Desvantagens
Melhoria na precisão ao remover o ser humano do processo de verificação	Custo da tecnologia associado
Redução dos custos eliminando um serviço terceiro na verificação da transação	Regulamentação estatal
Descentralização dificulta a adulteração de dados	Historial de uso ilícito
Segurança, eficiência e privacidade	

Figura 4 – Tabela de vantagens e desvantagens

A seguir serão descritas mais ao pormenor os fatores mais importantes presentes na tabela:

Transações privadas

Muitas redes blockchain operam como base de dados públicos, o que significa que qualquer pessoa com uma conexão à Internet pode visualizar uma lista do histórico de transações da rede. Embora os usuários possam acessar aos detalhes sobre as transações, eles não podem acessar ás informações de identificação sobre os utilizadores que fazem essas transações. É um equívoco comum que as blockchain são anónimas, quando na verdade são apenas confidenciais.

Custos associados

Embora o blockchain possa economizar dinheiro dos usuários em taxas de transação, a tecnologia está longe de ser gratuita. O sistema de "prova de trabalho" que a bitcoin usa para validar transações, por exemplo, consome grande quantidade de poder computacional. No mundo real, a energia dos

milhões de computadores na rede bitcoin é próxima à que a Dinamarca consome anualmente. Assumindo custos de eletricidade de $ 0,03 ~ $ 0,05 por quilowatt-hora, os custos de mineração exclusivos de despesas de hardware são cerca de $ 5.000 ~ $ 7.000 por moeda.

Aplicações da blockchain

Apesar da blockchain, como anteriormente demonstrado, estar mais relacionada com as cripto moedas e o setor financeiro esta pode ser aplicada em diversas outras áreas. Esta tecnologia também não deve ser implementada em qualquer tipo de negócio/aplicação devido ao seu alto custo energético/computacional. A seguir estão descritas algumas das áreas em que a blockchain já foi aplicada e obteve sucesso.

Cuidados de saúde

Cuidados de saúde

Os prestadores de cuidados de saúde podem aproveitar o blockchain para armazenar com segurança os registos médicos dos seus pacientes. Quando um registo médico é gerado e assinado, ele pode ser gravado na blockchain, o que fornece aos pacientes a prova e a confiança de que o registo não pode ser alterado. Esses registos pessoais de saúde podem ser codificados e armazenados na blockchain com uma chave privada, de modo que sejam acessíveis apenas por determinados indivíduos, garantindo assim a privacidade.

Cadeias de abastecedores

Um exemplo é o IBM Food Trust, os fornecedores podem usar a blockchain para registar as origens dos materiais que compraram. Isso permitiria às empresas verificar a autenticidade de seus produtos, junto com rótulos comuns como "Orgânico", "Local" e "Comércio justo".Conforme relatado pela Forbes, a indústria de alimentos está cada vez mais a usar a blockchain para rastrear o caminho e a segurança dos alimentos ao longo da jornada da fazenda ao usuário. Esta aplicação da blockchain pode ser implementada juntamente com um tipo de SI, o SCM para gerir as cadeias de abastecedores de uma empresa de forma mais segura e viável.

Atos eleitorais

Como mencionado, a blockchain pode ser usada para facilitar um sistema de votação moderno. Votar com a blockchain carrega o potencial de eliminar a

fraude eleitoral e aumentar a participação eleitoral, como foi testado nas eleições de meio de mandato de novembro de 2018 na Virgínia Ocidental, anteriormente mencionado na história da blockchain. Usar a blockchain dessa

forma tornaria os votos quase impossíveis de adulterar.
O protocolo do blockchain também manteria a transparência no processo eleitoral, reduzindo o

pessoal necessário para conduzir uma eleição e fornecendo aos funcionários resultados quase instantâneos. Isso eliminaria a necessidade de recontagens ou qualquer preocupação real de que uma fraude possa ameaçar a eleição.

Conclusões

Para concluir podemos afirmar que a blockchain é uma tecnologia cada vez mais em voga, já com provas mais que dadas em termos de segurança. Apesar disso podia ser uma tecnologia muito mais utilizada não fosse os entraves de regulamentação e custos tanto energéticos como computacionais referidos anteriormente.

Por último é bom referir que pode ser implementado em várias áreas, apesar disso quando pretendermos implementar uma blockchain devemos sobretudo fazer um estudo de custo benefício para verificarmos se realmente vale a pena implementar esta mesma tecnologia, pois podemos correr no erro de "estarmos a utilizar um canhão para matarmos uma mosca".

Bibliografia

- https://epocanegocios.globo.com/Tecnologia/noticia/2019/03/ataque-dos-51-como-funciona-pratica-que-coloca-em-duvida-seguranca-do-blockchain.html
- https://www.youtube.com/watch?v=93E_GzvpMA0&ab_channel=zlotolow
- https://academy.binance.com/pt/articles/history-of-blockchain
- https://foxbit.com.br/o-que-e-blockchain/