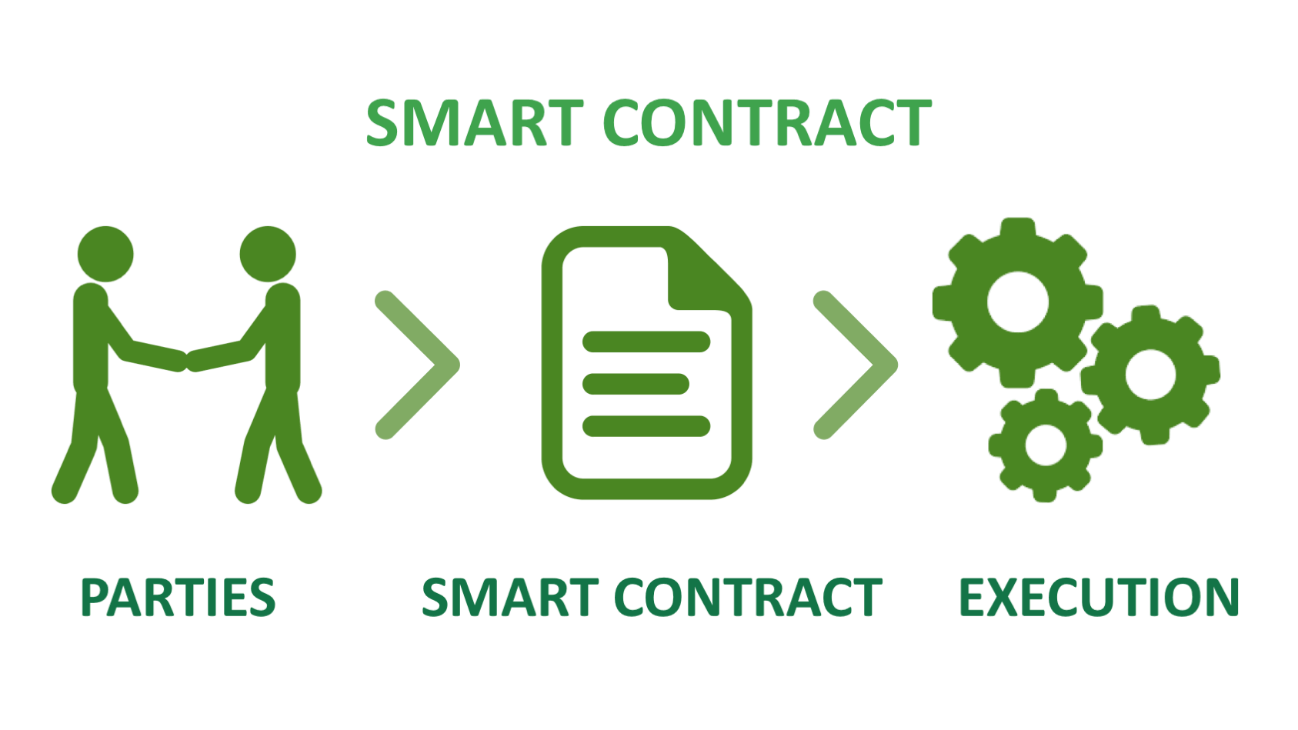
**Smart contracts**

Mestrado em Engenharia Informática

Criptografia 2021



Trabalho realizado por:

Marcelo Feliz nº50356

**Introdução**

Smart contracts são sistemas de contratos utilizados para executar transações automaticamente sem a necessidade da uma empresa, governo ou entidade para intermediar.

Em outras palavras, é uma condição imposta que, uma vez alcançada, executa automaticamente uma determinada transação.

Posto isto, um utilizador pode criar um contrato que simplesmente consista em enviar uma determinada quantidade de valor(algum tipo de cripto moeda) automaticamente por exemplo a uma determinada hora ou quando o valor de uma cripto moeda chega a um determinada valor.

Sendo assim, qual a diferença entre um contrato inteligente e um contrato “normal” que se costuma fazer tradicionalmente? Nos contratos convencionais, um documento determina os termos de uma relação entre duas partes, que são reforçadas pela lei. Se uma das partes não cumpre esses termos, a outra parte pode processar essa pessoa por não cumprir com o acordo.

No universo cripto, esse contrato estaria em uma blockchain e você não precisaria de instituições tradicionais do sistema para validar a operação, ou seja, é o que chamamos de descentralização que tem como princípio não dar o “poder” a ninguém ou a alguma instituição. Um contrato inteligente fortalece esses acordos com códigos e as regras são automaticamente aplicadas sem precisar de um terceiro.

**Rede de smart contracts**

Qual a diferença entre os contratos inteligentes da rede Bitcoin e da rede Ethereum? A rede Ethereum substitui a linguagem mais rudimentar do Bitcoin por uma que permite que desenvolvedores criem aplicações mais sofisticadas (Solidity), porque sua linguagem é muito mais amigável.

Mas é confiável? Bom, os contratos inteligentes são, sim, sujeitos a fraude. A rede Ethereum já presenciou perdas de milhões de dólares pela exploração de vulnerabilidades nos smart contracts. Mas essas falhas devem ficar cada vez menos comuns ao longo do tempo e os problemas de segurança devem sumir com o avanço da tecnologia.

O Bitcoin foi criado mais ou menos em [2008](https://investidorsardinha.r7.com/aprender/crise-2008-economia/), na época de uma das maiores [crises financeiras](https://investidorsardinha.r7.com/aprender/crise-financeira/) do mundo. Em janeiro de 2009, as primeiras transações começaram a ocorrer. O fundador da criptomoeda é anônimo e, após apresentar e explicar sobre o funcionamento do Bitcoin, não voltou a comentar.

Por outro lado, a plataforma Ethereum foi criada em 2013 e em 2015 foi posta no ar. O seu criador foi Vitalik Buterin, um programador canadense. O Ethereum foi financiado por um projeto de [crowdfunding](https://investidorsardinha.r7.com/aprender/financiamento-coletivo-o-que-e/). O fato de ter um criador conhecido significa que ele interfere na rede, mesmo que ele não a controle.

De maneira geral o Ethereum é considerado mais rápido do que o Bitcoin. Isso porque eles trabalham com tempos diferentes nos blocos da rede blockchain, que são as sequências de dados com informações sobre as transações. No Bitcoin existe um bloco a cada 10 minutos, em média. Já no Ethereum, o prazo é de apenas 13 segundos.

A [escalabilidade](https://investidorsardinha.r7.com/aprender/escalabilidade-investimentos/) e a velocidade com que as transações são registradas é um desafio tanto para o Bitcoin, quanto para o Ethereum. Apesar disso, como o Ethereum é mais flexível, ele já está tomando medidas com o objetivo de aumentar a velocidade da rede.

Dessa forma, diversas atualizações serão realizadas visando tornar a rede mais escalável e reduzir os custos das taxas. Já o Bitcoin é mais conservador e ainda precisa enfrentar esses problemas. Uma dessas soluções é a implementação de segunda camada que já está a ser desenvolvida a algum tempo mas ainda não tem data para ser utilizada, mas promete reduzir drasticamente o custo e tempo de transações na rede.

Outra diferença entre o Bitcoin e o Ethereum é que no Bitcoin os custos variam segundo o espaço que a transação irá ocupar no bloco. Já no Ethereum os custos variam de acordo com a complexidade da execução do contrato. Sendo que normalmente o Ethereum possui custos mais baixosmas ainda bastante elevados para a utilização recorrente dos utilizadores comuns, sendo um dos valores mínimos perto de 20dolares dependendo do nível de utilização da rede no momento.

**8 Vantagens dos Smart Contracts**

Na introdução já mencionei alguns dos aspectos chave dos contratos digitais que se baseiam em tecnologias de cadeia de bloqueio. Mas a lista de vantagens é mais longa, e dou algumas indicações para que seja mais fácil compreender porque é que os Contratos Inteligentes têm um potencial tão grande.

**1. Confiança**

Em cada transacção é importante ter confiança para ambas as partes que esta transacção funcione realmente. Devido à forma única de armazenar informação na cadeia de bloqueio, muitos computadores partilham a informação e verificam-na indipendentemente, é possível utilizar o chamado “livro-razão distribuído” de que esta informação é válida e também não se pode perder. Assim, o contrato também existirá no futuro e não será alterado.

**2. Cópia de segurança**

Devido à mecânica de armazenamento da informação no livro-razão distribuído, é também importante mencionar que existem muitas cópias na rede. Isto garante um backup redundante de todos os documentos criados e de todos os contratos aplicados.

**3. Autonomia**

Uma vez que a rede está a tratar da entrega e dos termos do contrato, é totalmente autónoma. Para uma transacção bem-sucedida, não é necessário um banco, corretor, advogado, regulador ou outros intermediários. Desta forma, pode estabelecer os seus próprios contratos e não está limitado por limitações ou custos locais envolvidos na verificação da transacção.

**4. Velocidade**

Os contratos tradicionais podem levar muito tempo a processar, verificar ou mesmo enfoce com terceiros. As Redes baseadas em cadeias de blocos podem acelerar este processo para apenas algumas horas ou transacções quase em tempo real. Isto é especialmente improvável quando se tem pequenas transacções que é necessário verificar rapidamente (Pense em alugar um carro, seguro de viagem, etc.)

**5. Custo**

Pode imaginar que os contratos que não necessitam de notário ou de testemunhas são menos dispendiosos. Isto também é aplicável para os Contratos Inteligentes. Quando os contratos estão a ser executados e verificados pela rede em vez de por terceiros, o custo por transacção torna-se mais baixo. Isto é especialmente importante para compreender se estiver à procura de “tokenize” activos. Onde se dividem grandes projectos em pequenos pedaços. (por exemplo, compra de uma parte de uma casa)

**6. Automação**

Uma grande vantagem de um Smart contract é que eles são “inteligentes”. Isso significa que também pode assegurar que estruturas complexas de contratos são cumpridas e que tem uma rastreabilidade do documento, mas também dos bens. Um exemplo envolve a expedição internacional, onde as mercadorias fluem através de diferentes legislações, atravessam diferentes fronteiras, são seguradas com diferentes seguradoras e todas precisam de ser geridas num contrato de modo a que a sua legibilidade seja garantida. Isto geralmente envolve contratos longos e muita papelada – que poderia ser automatizada e rastreada com um Contrato Inteligente.

**7. Criptografia e Segurança**

Outro papel importante é, evidentemente, a transacção segura. Isto não significa apenas que o documento e o contrato são armazenados de forma redutora, mas também que a informação só é acessível quando alguém é autorizado. A utilização de protocolos de rede e criptografia muito seguros, juntamente com outros níveis de segurança, assegura que apenas as partes envolvidas podem aceder à informação.

**8. Exatidão dos contratos**

Por último, mas não menos importante, pode haver muitos erros quando se lida com intermediários ou quando se lida com papelada manual. Isto pode ser um pequeno factor, mas também vale a pena mencionar, que existe uma melhor visão geral e, portanto, também uma melhor precisão para os contratos aplicados.

**Lado negativo dos contratos inteligentes**

Claro que estão longe de ser perfeitos e como se baseia em software, existem também problemas como potenciais bugs, custo da rede, etc.

Outra coisa a mencionar é a regulamentação em falta neste momento. Atualmente não existem orientações e leis reais que regulem os contratos inteligentes. Isto significa que também não existe qualquer cópia de segurança. Quando estiver a alugar o seu carro com um contrato de bloqueio automático, houve um erro no pagamento, então o seu carro pode não estar acessível ou mesmo ser alugado à próxima pessoa antes de poder reagir – lembre-se, não há nenhum intermediário que possa mediar.

Também vale a pena mencionar que estes contratos funcionam, não importa o que aconteceu. Se estabelecer as condições erradas, ele executará, não importa o que aconteceu.

Isto também é verdade com a privacidade dos dados. No lado positivo está o facto de não haver dados perdidos na Blockchain, mas quando se trata de dados pessoais, pode ser também um lado negativo. Este é ainda um problema não resolvido e aberto, que os dados pessoais não podem ser apagados.