Introdução

Desde os pensamentos teóricos em um tempo que era impossível aplicar aquilo que estava sendo teorizado até quando tais teorias foram de fato implementadas, a computação sempre foi vista como revolucionária mudando a maneira que vivemos e como enxergamos determinados nichos que estavam estagnados à séculos. Uma revolução que estamos presenciando atualmente é no nicho econômico, com a chegada das criptomoedas e dos contratos inteligentes. Tecnologias disruptivas que mudaram completamente a visão de mercado, em como os indivíduos realizam trocas voluntárias sem se submeter à alguma entidade.

Com menos de uma década de desenvolvimento, as criptomoedas impactaram a economia tradicional, mudando a visão centralizada que muitos economistas clássicos tinham sobre o conceito de 'moeda'. Apesar de serem aplicados com eficiência recentemente, os conceitos por trás das criptomoedas e contratos inteligentes já existem desde a década de 1990.

Os contratos inteligentes ao se mostrarem independente de um mediador e, por tanto, livre das taxações e limitações e impostas por ele, acabam barateando, agilizando e dando mais liberdade para as partes entrarem em um consenso que melhor atenda às suas condições. Este barateamento no processo de troca em um sistema de livre comércio com concorrência, pode acabar interferindo diretamente no preço do produto final.

Desenvolvimento

O conceito de uma criptomoeda não é algo recente, a Bitcoin (2009), ao contrário do que muitos pensam, não foi a primeira criptomoeda a surgir, houveram várias outras tentativas como a DigiCash (1989) e a Bit Gold (1998). O surgimento da Bit Gold, desenvolvida por Nick Szabo, foi um marco notório pois utilizava a tecnologia Blockchain que é base para as criptomoedas atuais, muitos a consideram como a percursora da Bitcoin.

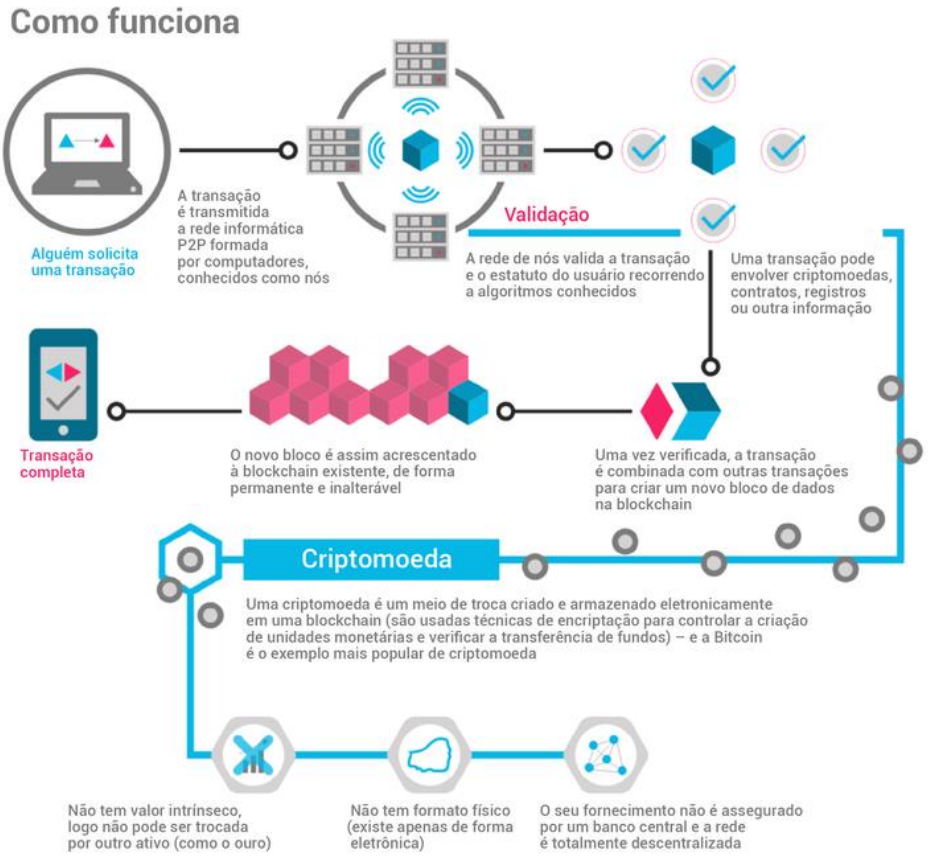
Blockchain

Conceito originalmente criado em 1991 que tinha como objetivo ser uma base de dados que usa a descentralização como medida de segurança e onde é possível consultar, adicionar mas não remover nem alterar os dados presentes. Como o nome sugere, blockchain é uma cadeia de blocos onde cada bloco possui o seu registro (dados), o hash do próprio bloco e o hash do bloco anterior.

Para garantir a propriedade de não poder remover ou alterar os dados, o blockchain possui camadas de segurança. Caso o registro do bloco seja alterado, o seu código hash também é alterado, fazendo com que o bloco posterior não tenha mais acesso à ele, quebrando a cadeia. Mas atualmente os computadores conseguem realizar milhares de cálculos por segundo, podendo assim, calcular os novos valores de hash para toda cadeia para validá-la. Para prevenir isso, a blockchain tem o Proof-of-work.

Com o seu conceito criado em 1993 com o objetivo de impedir spam de e-mails, o proof-of-work é um mecanismo que basicamente desacelera a criação de novos blocos. Caso um bloco da cadeia seja alterado, será preciso calcular o proof-of-work para todos os outros blocos seguintes na cadeia. Além do uso conjunto dos hashes e do proof-of-work, o blockchain é distribuído o que contribui para manter a cadeia segura.

O blockchain usa uma rede P2P, quando uma nova pessoa entra na rede, ela recebe uma cópia da cadeia. Quando um novo bloco é criado, ele é enviado para todos os nós da rede para que cada nó verifique se o bloco foi adulterado, caso seja aprovado, cada nó adiciona o novo bloco na sua rede.



Com todas essas camadas de segurança, para adulterar um bloco na cadeia seria preciso controlar mais de 50% da rede P2P, calcular o proof-of-work e recalcular os hashes para todos os blocos seguintes na cadeia, o que é quase impossível de acontecer.

O próprio cálculo do proof-of-work requer um grande custo computacional e elétrico, o que acaba dando vantagem, para quem possui os melhores equipamentos, na criação de um novo bloco. Além disso, os mineradores também se juntam às chamadas “mining pools”, que são um conjunto de mineradores que combinam seu poder computacional e distribuem a recompensa uniformemente, o que acabaria tirando o conceito “distribuído” do blockchain. Surgiram várias proposições para contornar isso, como por exemplo o proof-of-stake.

O conceito do proof-of-stake surgiu pela primeira vez em 2011 em uma postagem no fórum Bitcointalk. O conceito se baseia em que a disputa entre os nós para conseguir calcular o novo hashe é inútil e parte de um princípio de escolha “aleatória” de um dos nós para validar o novo bloco a ser adicionado na blockchain.

No proof-of-work, os nós não são escolhidos de maneira realmente aleatória, o nó precisa adicionar uma quantidade de moedas à rede para poder se tornar um validador. A quantidade de moedas depositadas influencia nas chances daquele nó ser escolhido para validar o próximo bloco, quanto mais moedas depositadas, maior é a chance do nó. Ao ser escolhido, o nó verificará se as transações, referentes ao novo bloco, são válidas e receberá as taxas que estão associadas à tais transações. O nó perderá parte de suas moedas depositadas caso aprove uma transação fraudulenta, diminuindo assim, suas chances de ser escolhido novamente.

No proof-of-stake é mais difícil de conseguir controlar mais da metade da rede, dependendo do valor da moeda. Usando a bitcoin como exemplo, custaria em torno de 79 bilhões de dólares para controlar mais da metade da rede.

Outro potencial problema do proof-of-work é na escolha dos nós já que é levado em consideração a quantidade de moedas que o nó adicionou na rede, o que poderia acabar por beneficiar os mais ricos que teriam mais chances de serem escolhidos, se tornariam mais ricos e assim teriam mais chances de serem escolhidos novamente. Uma das possíveis soluções para esse problema seria levar em consideração a “idade” das moedas do nó.

Mais um potencial problema do proof-of-stake seria o nó escolhido como validador não analisar as transações do novo bloco para assim poder validá-lo. Uma das possíveis soluções para esse problema seria selecionar, também, outros nós como validadores reservas.

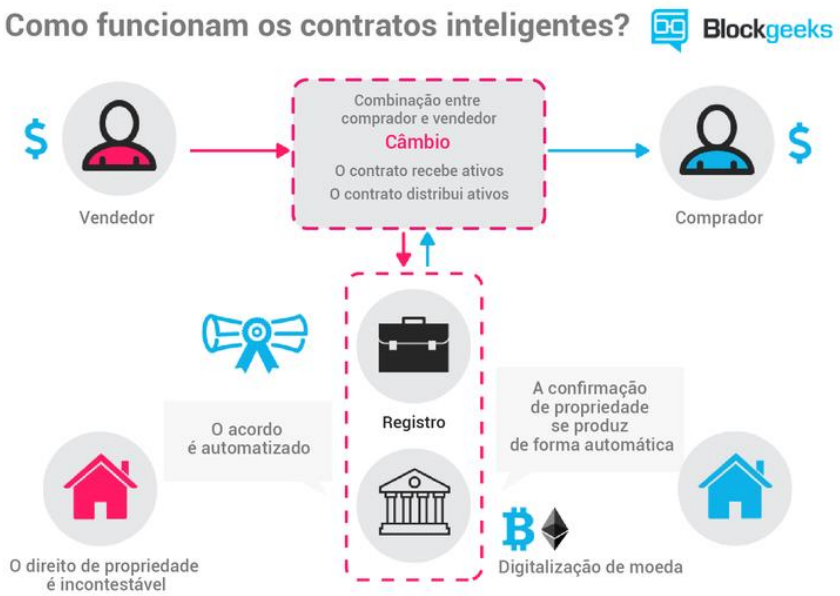
Em resumo, proof-of-stake é um conceito ainda muito novo que pode vir a substituir o proof-of-work. Mas, como em qualquer nova tecnologia, ainda traz riscos que precisam ser estudados e solucionados. Já existem moedas que se utilizam do sistema de proof-of-stake, como por exemplo a Etherium que está desenvolvendo um sistema de proof-of-stake denominado Casper.

O blockchain ainda é considerado uma tecnologia recente e que está em constante evolução e que a cada dia surgem mais utilidades práticas para problemas reais. Além das criptomoedas, uma das criações recentes que se apoiam no uso do blockchain, são os contratos inteligentes.

Contratos Inteligentes

O termo “smart contracts” foi primeiramente utilizado por Nick Szabo um jurista, criptógrafo e cientista da computação, o mesmo procurava por uma maneira segura e distribuída de armazenar contratos. Por utilizar uma forma de armazenamento descentralizada, a segurança do contrato é garantida pela tecnologia blockchain, ou seja, precisam ser validados em uma rede P2P e não podem ser alterados após sua criação. Contratos Inteligentes são programas escritos que estabelecem as mesmas características dos contratos reais. O contrato pode ser cumprido e executado de forma automática sem a necessidade de um terceiro mediador.

Os contratos inteligentes funcionam de maneira similar à um sistema de crowdfunding, onde as partes presentes são as pessoas que querem apoiar um projeto e as pessoas que vão realizar o projeto. As pessoas que querem apoiar o projeto colocam o dinheiro que é armazenado e é passado automaticamente para a equipe do projeto caso algum evento, condição ou objetivo seja alcançado e retorna para as pessoas que apoiaram caso o contrário. A diferença dos contratos inteligentes para um crowdfunding é que não se faz necessário uma empresa mediar o processo.



A maioria das compras pessoa-a-pessoa realizadas na internet acontecem por meio de um mediador (Mercado Livre, eBay, Bancos), por causa da falta de confiança. Estes mediadores cobram taxas e acabam impondo limitações nas maneiras de realizar trocas, o que acaba sendo um empecilho em um sistema de troca voluntária e livre mercado.

Ao contrário dos contratos reais escritos em linguagem jurídica, os contratos inteligentes não dão margem para diferentes interpretações, não dependem de um mediador para ser validado e não estão sujeitos à um sistema judicial público que é caro e lento. O uso dos contratos inteligentes barateia o processo da troca, onde em um sistema de concorrência (livre mercado) isso impactaria no preço final do produto ou serviço. Por não estar sujeito as limitações de um mediador, as partes têm total liberdade para ajustar as condições do contrato de maneira que atenda o melhor possível à todos.

Moeda Fiduciária

Moeda fiduciária é sem lastro e não possui valor intrínseco. Seu valor depende exclusivamente da confiança das partes em quem a emitiu. É qualquer ordem de pagamento como cheques e dinheiro em papel. Foi o modelo de dinheiro que substituiu o padrão-ouro no mundo.

Dado um produto na economia, quanto mais ofertas existirem para este produto, seu preço (relação de troca com o dinheiro) seria alterado consideravelmente. Da mesma maneira, quanto mais dinheiro, menor é o seu valor de troca. Para algo ser usado como dinheiro precisaria ser difícil de falsificar, possuir um valor (aceitação por uma quantidade considerável de pessoas), fácil de transportar e ser escasso. A moeda é algo que é aceitado como dinheiro em uma determinada região, podendo assim caracterizar uma transação entre partes.

Dado este contexto, a moeda fiduciária se mostra inconsistente dado que está atrelada à algum tipo de governo que pode emitir à vontade, tirando assim a característica da escassez e podendo gerar uma inflação.

Criptomoedas

É uma moeda digital que, ao contrário dos sistemas bancários centralizados, se utiliza do blockchain e da criptografia para validar uma transação e a criação de novas unidades da moeda de maneira descentralizada. A primeira moeda digital descentralizada criada foi a Bitcoin em 2009 por Satoshi Nakamoto (pseudônimo), e a quantidade máxima que irá circular já foi determinada desde a sua criação, para assim garantir a propriedade da escassez.

No ano passado a Bitcoin teve o seu boom chegando a valer U$ 20.000 a unidade. Alguns economistas apontaram como bolha, enquanto que outros rebatiam com o argumento de que a bitcoin ainda não tem uma circulação alta o suficiente para possuir um valor intrínseco dado que a definição de bolha econômica é quando algo na economia passa a valer mais do que o seu valor intrínseco sem qualquer motivo aparente. Hoje a maior parte das pessoas enxergam a Bitcoin como um investimento, enquanto que outros já a usam como moeda e a enxergam como uma maneira de se proteger dos modelos inflacionários das moedas fiduciárias.

A criptomoeda se torna mais poderosa quando usada em conjunto aos contratos inteligentes, a primeira criptomoeda a suportar tal funcionalidade foi a Bitcoin. Mas ainda eram contratos básicos, já que se restringia à transação da moeda entre pessoas. A Etherium chegou com uma proposta que visa dar liberdade para os desenvolvedores escreverem seus próprios contratos através de uma linguagem turing-complete que, ao contrário da Bitcoin, suporta um conjunto amplo de instruções. A linguagem adotada nos contratos inteligentes da Etherium é a Solidity cuja sintaxe é similar à JavaScript.

Conclusão

As criptomoedas ainda são vistas pela grande maioria como um investimento e não como uma moeda. Ainda é preciso se difundir como moeda, para assim conseguir um valor intrínseco e se tornar mais comum nas transações entre pessoas. Ainda se tem um certo receio por parte das pessoas, já que o senso comum aceita mais facilmente a moeda fiduciária, mas isso é algo comum em novas tecnologias, precisam de tempo para se aperfeiçoarem e se difundirem.

Os contratos inteligentes vão muito além do uso conjunto com criptomoedas, o simples conceito de algo ser executado de forma automática caso algum evento ocorra ou objetivo seja alcançado, já se mostra eficiente para resolver problemas comuns, para agilizar e baratear o custo que se tem no processo tradicional.

As criptomoedas e contratos inteligentes chegaram revolucionando a maneira em como os indivíduos realizam trocas, mas ainda é uma tecnologia que está engatinhando e que tem um grande potencial para revolucionar ainda mais a visão que temos sobre economia e assim olharmos para o passado e pensarmos o quão o modelo anterior era primitivo.

Referências

Wikipedia. Criptomoeda. 2018. Disponível em: <https://pt.wikipedia.org/wiki/Criptomoeda>. Acesso em: 24 Out. 2018.

Criptomoedas e criptoativos criam uma nova economia mundial. 2018. Disponível em: <http://tiinside.com.br/tiinside/home/internet/17/05/2018/criptomoedas-e-criptoativos-criam-uma-nova-economia-mundial/>. Acesso em: 24 Out. 2018.

Bitcoin e o impacto da tecnologia blockchain na economia mundial. 2018. Disponível em: <https://www.hsm.com.br/bitcoin-e-o-impacto-da-tecnologia-blockchain-na-economia-mundial/>. Acesso em: 24 Out. 2018.

CARDOSO, Bruno. Contratos Inteligentes: descubra o que são e como funionam. 2018. Disponível em: <https://brunocardosoadv.com/contratos-inteligentes/>. Acesso em: 24 Out. 2018.

LIMA, Raphaël. Criptomoedas: libertando pessoas do complexo bancário-estatal. 2018. Disponível em: <https://cointimes.com.br/criptomoedas-libertando-pessoas-do-complexo-bancario-estatal/>. Acesso em: 24 Out. 2018.

Examinando a história da criptomoeda – Como evoluiu desde o início até agora. Disponível em: <https://www.criptonario.com.br/examinando-historia-da-criptomoeda/> Acesso em: 24 Out. 2018.

Wikipedia. Blockchain. 2018. Disponível em: <https://pt.wikipedia.org/wiki/Blockchain>. Acesso em: 24 Out. 2018.

IORIO, Ubiratan Jorge. A teoria monetária austríaca. 2010. Disponível em: <https://www.mises.org.br/Article.aspx?id=697>. Acesso em: 24 Out. 2018.

Smart Contracts: The Blockchain Technology That Will Replace Lawyers. Disponível em: <https://blockgeeks.com/guides/smart-contracts/>. Acesso em: 24 Out. 2018.

MISES, Ludwig von. As Seis Lições. 7. Ed. São Paulo: Instituto Ludwig von Mises Brasil, 2009

Simply Explained – Savjee. How does a blockchain work. 2017. Disponível em: <https://www.youtube.com/watch?v=SSo_EIwHSd4>. Acesso em: 24 Out. 2018.

Simply Explained – Savjee. Smart contracts. 2017. Disponível em: <https://www.youtube.com/watch?v=ZE2HxTmxfrI>. Acesso em: 24 Out. 2018.

Simply Explained – Savjee. Proof-of-Stake (vs proof-of-work). 2018. Disponível em: <https://www.youtube.com/watch?v=M3EFi_POhps>. Acesso em: 24 Out. 2018.

Wikipedia. Moeda Fiduciária. 2018. Disponível em: <https://pt.wikipedia.org/wiki/Moeda_fiduci%C3%A1ria>. Acesso em: 24 Out. 2018.