Criptomoedas: Bitcoins, Altcoins e Blockchain

GRUPO 8

Cristiano Jóse Furlan, Matheus Cumpian, Lorenzo Villas Boas e Igor Gouvea

Faculdade de Tecnologia – Universidade Estadual de Campinas

SI 102 – Seminários 1

Abstract. *This report aims to present the topics of Blockchain, Altcoins and Blockchain, presenting basic concepts of functioning and showing their presence in daily life, with news and works on the subject, addressing history, advantages and disadvantages, news and technical concepts of the theme.*

Resumo. *Este relatório tem como objetivo apresentar os tópicos de Blockchain, Altcoins e Blockchain, apresentando conceitos básicos de funcionamento e mostrando sua presença no cotidiano, com noticias e trabalhos a respeito do tema, abordando história, vantagens e desvantagens, notícias e conceitos técnicos do tema.*

1. História

A história das criptomoedas revela um desafio central do dinheiro: como desenvolver um sistema que possa efetivamente facilitar o intercâmbio de bens e serviços ao mesmo tempo que gera prosperidade e impede que as instituições que o administram abusem da confiança decorrente dessa função

As criptomoedas, diferente das moedas reais, não emitidas por algum governo, que de alguma forma as lastreia, mas é emitida por um conjunto de usuários que concordem sobre o valor que ela tem. Na verdade as moedas reais também funcionam desta maneira. A grande diferença é que a respeito das moedas reais, nós usuários concordamos em um valor relativamente estável.

As primeiras moedas virtuais tinham, contraintuitivamente, existência física. Você precisa voltar até 1896 para encontrar a primeira, que era chamada Selo S&H e foi lançada pela empresa Sperry and Hutchins. Os selos S&H eram vendidos em postos de gasolina e em supermercados que os davam como bonificação aos compradores que podiam então resgatar mercadorias específicas em um catálogo da S&H. Nos anos 60, a empresa tinha emitido 3 vezes mais selos que o serviço postal dos EUA.

American Advantage teve início em 1981 quando a American Air Lines lançou o American Advantage (AAdvantage), que foi o primeiro programa de milhagens aéreas.

Hoje, toda companhia aérea e até mesmo empresas de aluguel de carros e a maior parte dos hotéis (EUA) oferecem alguma versão do programa de milhagem. Em 2005, a revista The Economist estimou que o valor total das milhas não resgatadas valia mais que todas as cédulas de dólar em circulação. As milhas aéreas são vendidas a preços razoáveis por milha e podem ser gastas em um número crescente de estabelecimentos e em uma infinidade de serviços – até mesmo para pagar por funerais! Ao longo dos últimos dez anos, as companhias aéreas fizeram mais dinheiro vendendo essa moeda virtual para companhias de cartões de crédito e hotéis do que realmente fizeram pelos voos em si.

No final de 2008, duas novas moedas de alto potencial foram lançadas. Bitcoin e Facebook Credits. Ambas apresentaram propostas para resolver os problemas de segurança das tentativas anteriores, mas de maneiras totalmente distintas. O Facebook Credits enfrentou uma morte prematura em 2012, não por causa de segurança ou fraude, mas porque só podia ser gasto dentro do Facebook, que na época era bem menor do que é hoje.

Em outubro de 2008 o pseudônimo de SatoshiNakamoto lançou um artigo técnico na Internet em que ele propôs uma versão puramente ponto-a-ponto do dinheiro eletrônico e que garantia a segurança através de sofisticada técnica de encriptação baseada em um modelo matemático. Assim nasceu o Bitcoin, uma criptomoeda segura e um sistema de pagamento online baseado em protocolo de código aberto que é independente de qualquer autoridade central.

A Bitcoin foi criada no dia 31/10/2008 no auge da crise mundial, por um programador desconhecido até hoje, usando o pseudônimo de SatoshiNakamoto. O qual publicou uma mensagem em um site de discussão online sobre criptografia o seu sistema de dinheiro eletrônico peer-to-peer. Nessa mensagem ele anexou um paper com nove páginas onde descrevia o funcionamento do sistema e suas características. Mas a pergunta que fica é: O Bitcoin surgiu do nada? Aparentemente sim, entretanto ele foi resultado de anos de intensa pesquisa e desenvolvimento por pesquisadores até os dias de hoje, anônimos. Sendo uma invenção revolucionaria na área da ciência da computação, tendo os inventores pesquisado e estudado o desenvolvimento de moedas criptografadas por cerca de 20 anos, e aproximadamente 40 anos pesquisado sobre criptografia.

O criador do Bitcoin é considerado um dos 50 mais ricos do mundo.O motivo para Nakamoto não estar na lista dos bilionários é que, mesmo oito anos depois do lançamento do bitcoin, a identidade de Nakamoto ainda é um mistério. Entre os suspeitos estão o estudante de criptografia Michael Clear; o professor de Economia Virtual de Oxford, Vili Lehdonvirta; e o trio de inventores Vladimir Oksman, Charles Bry.

Um empresário australiano, Craig Steven Wright, foi preso em 2015 por sonegar impostos e chegou a alegar ser Nakamoto. O empresário chegou a ser identificado pela revista "Wired" e pelo "Gizmodo", mas esse fato ainda não foi totalmente comprovado. Wright foi incapaz de assinar criptograficamente o primeiro bloco de dados gerados com a criptomoeda, coisa que o verdadeiro Satoshi Nakamoto seria capaz de fazer.

No momento de sua publicação nenhum especialista acreditava no sucesso, pois já tinham tentado criar outras criptomoedas, porém em todas as oportunidades não tiveram êxito. A grande maioria afirmava que a moeda teria problemas em sua seguran

No dia 03/01/2009, mais precisamente as 18:15 nascia o Bitcoin e sua primeira transação, feita por Satoshi, onde foram geradas 50 BTC, as quais foram registradas no primeiro bloco, o bloco gênese do blockchain. Esta primeira transação foi acompanhada de uma mensagem que fazia alusão a uma manchete do jornal americano The Times. Nela, Satoshicriticava o sistema bancário e a instabilidade financeira da época, causada pelo monopólio estatal com suas grandes intervenções na economia.

LaszloHanyecz foi conhecido por fazer a primeira transação documentada em que Bitcoin foi usado para comprar um item físico.

Em 22 de maio de 2010, Hanyecz pagou 10.000 BTC para outra pessoa lhe pedir duas pizzas. Esta transação foi considerada a primeira em que um vendedor aceitou o pagamento em Bitcoin por um item físico.

É impossível negar o sucesso que o bitcoin teve. Apesar do bitcoin estar sofrendo com alguns problemas que precisam ser abordados, como escalabilidade e privacidade, a Moeda Digital tornou-se a principal criptomoeda do mundo. O bitcoin foi projetado para possibilitar transações globais e aumentar a inclusão financeira. Além disso, milhares de comerciantes em todo o mundo começaram a aceitar pagamentos em bitcoin, tanto no mundo on-line e off-line.

Hoje, uma unidade de Bitcoin vale aproximadamente 33500 reais

Embora o crescimento da popularidade do Bitcoin e da tecnologia blockchain tenha sido nada menos que explosivo, o desenvolvimento da escalabilidade está sendo muito lenta se compararmos com a rápida valorização do bitcoin nesse ano de 2017, uma vez que já foi limitado um número máximo de 21 milhões de bitcoins circulando, e já existem 17 milhões. E isso tem de fato, afetado seriamente o desenvolvimento do Bitcoin, e ameaçado seu status como ‘rei das criptos’ e dando a outras moedas e tecnologias a oportunidade de acelerar sua expansão.

2. Blockchain

O blockchain é uma rede de negócios segura, na qual os participantes transferem itens de valor (ativos), por meio de um ledger (livro-razão) comum distribuído, do qual cada participante possui uma cópia, e cujo seu conteúdo está em constante sincronia com os outros. É importante destacar que existem diversas redes Blockchain, além da rede do Bitcoin, como a do Ethereum, Hyper Ledger, Ripple etc., e todas elas funcionam paralelamente.

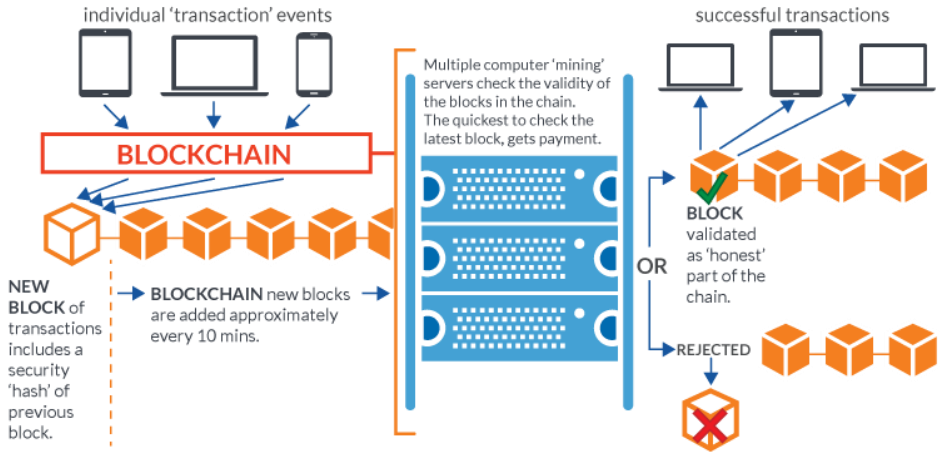
A arquitetura Blockchain tem como característica a comunicação entre dois ou mais nós (computadores) que compõem uma rede Peer-to-peer (P2P).

“Peer-to-peer (do inglês par-a-par ou simplesmente ponto-a-ponto, com sigla P2P) é uma arquitetura de redes de computadores na qual cada um dos pontos ou nós da rede funciona tanto como cliente quanto como servidor, permitindo compartilhar serviços e dados sem a necessidade de um servidor central.” - Wikipedia

Na arquitetura Blockchain, as informações de todas as transações já realizadas são enviadas para um livro-razão, que funciona como um banco de dados ou planilha Excel,

como preferir, e nada pode alterar os dados que estão lá. Todos os nós têm uma cópia idêntica desse livro-razão, logo, todos têm a mesma informação.

As transações são dadas por chaves públicas e privadas, onde as chaves privadas são a assinatura de autenticidade e as chaves públicas são os “endereços” das carteiras.



Funcionamento da Blockchain – Imagem 1

Os blocos da blockchain são validados pelos mineradores, os mineradores são seeders da rede p2p que estão costantemente baixando e enviando dados da blockchain, eles tem como tarefa a validação do hash correspondente a cada bloco novo inserido. Basicamente os blocos tem um "nome" esse nome é o nonce do bloco, o minerador deve descobrir a hash do bloco que corresponde ao nonce e o conteúdo presente do bloco, adicionados mais um certo valor de zeros antes da hash, o número de zeros é a chamada difilcudade da
rede.

Estrutura de um bloco – Imagem 2

Devido aos mineradores, a blockchain se torna uma forma muito segura de guardar dados, já que todos os dados são validados desde o ínicio da "corrente", e nenhum dado pode ser alterado sem que todos os outros sejam alterados também, visto as ligações de hashs entre blocos.

3. Altcoins

Altcoins são moedas digitais criadas a partir de uma tecnologia semelhante a do bitcoin.

Altcoins – Imagem 3

Abaixo eu citei algumas das principais criptomoedas usadas no mercado e seu tipo de uso:

LITECOIN

É considerado apenas uma cópia do bitcoin porém o litecoin oferece um algoritmo de mineração diferente permitindo transações mais rápidas. Entretanto o litecoin possui uma maior rejeição no mercado do que em relação ao bitcoin.

ETHEREUM

Foi instituída no mercado em 2013 e desde então existe no mercado uma grande comparação entre a ethereum e o bitcoin porém elas se organizam de forma diferente já que a Ethereum se concentra em desenvolver blockchains, com tokens nativos, contratos inteligentes e aplicações descentralizadas que não necessitam de intermediários podendo assim interagir com sistemas sociais, financeiros, interface de jogos e qualquer outra coisa.

RIPPLE

Foi desenvolvida em 2012 e o foco principal da Ripple não é ser uma moeda de especulação igual a maioria de outras criptomoedas e com isso ela tem atraído a atenção de vários bancos ao redor do mundo que buscam investir nessa área. E esses ideais são praticamente opostos aos propostos pelo bitcoin que pretendia diminuir a hegemonia do sistema financeiro atrelado aos bancos, que surgiu em 2009 após a grande crise de 2008.

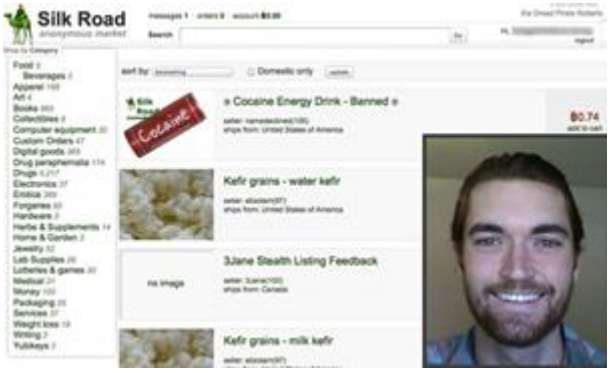
MONERO

Foi uma moeda criada em 2014 que foca em privacidade em descentralização e isso acaba garantindo o anonimato de seus usuários e através disso acabou atraindo mercados da darknet.

DASH

Foi implantada em 2013 e em relação as outras moedas possui as transações mais rápidas e em questões de segundos as trocas podem ser concluídas. Ela permite estas trocas rápidas pois é uma moeda descentralizada o que permite trocas sem a necessidade de uma autotização nas trocas.

AÇÕES ILEGAIS ASSOCIADAS A CRIPTOMOEDAS



Silk Road – Imagem 5

Um dos problemas que surgiram com as criptomoedas foi a dificuldade de localizar os seus usuários e com isso muitos usuários começaram a usar o sistema de maneira ilegal e como exemplo é possível citar o caso da empresa virtual chamada de Silk Road que foi um site inaugurado em 2011 que vendia drogas com o uso de bitcoins e o FBI encontrou grandes dificuldades para desmascarar o anonimato do dono desse site e após 2 anos conseguiram identificar Dread Pirates Roberts (pseudônimo) do dono do site que era comandado por Ross Ulbricht de 29 anos que movimentou mais de 1,3 de bilhão de dólares em bitcoins.

4. Vantagens e desvantagens

VANTAGENS:

AGILIDADE NAS TRANSFERENCIAS

As transações com bitcoins são mais rápidas do que outros meios digitais. Em uma transação comum, o envio da criptomoeda de uma carteira digital para outra costuma durar entre 10 e 25 minutos. Para efeitos comparativos, uma transação bancária entre contas de um mesmo banco demora cerca de meia hora, uma transferência TED até uma hora e um envio internacional de dinheiro pode demorar mais de três dias úteis.

SISTEMA INTERNACIONAL

No sistema bancário brasileiro, enviar dinheiro para fora do país ou pagar uma despesa internacional costuma ser uma tarefa complicada. Enquanto a economia mundial e as trocas internacionais cresceram largamente nas últimas décadas, o sistema financeiro não se adaptou ao ritmo de mudança.

As criptomoedas quebram essas barreiras artificiais e atuam em escala global. É possivel enviar criptomoedas para qualquer pessoa do mundo pagando as mesmas taxas e demorando o mesmo tempo de uma transação para uma pessoa que está do outro lado da rua. O tempo da transação ainda seria mais rápido do que o tempo gasto para realizar a mesma transação usando o sistema bancário tradicional.

SEGURANÇA

A segurança de um banco depende totalmente na confiança que seu cliente tem nele, os clientes devem confiar que o banco não irá quebrar ou frauda-los, que a operadora do cartão não será hackeada e confiar que o governo não irá congelar ou confiscar os seus ativos financeiros. Infelizmente, a história financeira é repleta de acontecimentos nesse sentido.

Contrariando essa situação, as criptomoedas não necessitam da confiança em pessoas, bancos, governos ou qualquer outro tipo de intermediário financeiro. Elas funcionam com base na criptografia, na descentralização e na matemática. A segurança se baseia no registro público de transações na Blockchain.MATHEUS ADICIONA ALGO SOBRE BLOCKCHAIN AQUI SE QUISER. Como o poder computacional da rede das criptomoedas está descentralizado em vários mineradores, é praticamente impossível hackear o sistema.

DESVANTAGENS:

VOLATILIDADE

O poder aquisitivo das criptomoedas é muito volátil quando comparado as moedas normais como o Real ou o Dólar. A diferença das moedas convencionais, que são armazéns estáveis de valor, o valor da Bitcoin, por exemplo, não está garantido. O porta-voz da Fundação Bitcoin, Jinyoung Englund previne, "estivemos dizendo todo o tempo que os investidores não deveriam investir mais no Bitcoin do que estão dispostos a perder".

POPULARIDADE

Ainda são poucos os estabelecimentos em que podemos usar criptomoedas como forma de pagamento. No Brasil, mais especificamente, o uso da moeda ainda é praticamente desprezível. Da mesma forma, há poucos usuários da moeda, para que faça sentido a aceitação em massa por empresas. E quem aceitasse ainda teria que convertê-las para reais, pelo menos em parte, para arcar com seus custos (fornecedores, salários, etc.). Além disso a volatilidade das criptomoedas dificultam sua adoção em comércios, visto que a variação de seu preço pode prejudicar empresas e faze-las perderem dinheiro na venda de seus produtos e serviços.

IMPACTOS AMBIENTAIS

Essa desvantagem une dois mundos que até então pareciam distantes, finanças e meio ambiente.

O Financial Times descobriu que cada transação em Bitcoin consome cerca de 215 kwh para ser processada e isso equivale ao que uma família inteira norte-americana consome em uma semana. O jornal ainda desta que como o Bitcoin e outras criptomoedas estão ganhando cada vez mais popularidade, mais cedo ou mais tarde, o debate sobre a sustentabilidade se tornará inevitável.

Isabella Kaminska, do Financial Times, explica o assunto:

"Quanto mais bitcoin se torna útil como uma ferramenta de troca, mais caro é manter e dinamizar sua gestão. É uma situação embaraçosa para os investidores que hoje estão cada vez mais conscientes das implicações ambientais, sociais e de governança corporativa de suas decisões ... Se o consumo de eletricidade for combinado com alguns medos sobre a opacidade da governança bitcoin, uso potencial para crimes cibernéticos ou operações do mercado negro, que, do ponto de vista daqueles que querem fazer investimentos responsáveis, as criptomoedas podem causar preocupação."

Referências

http://fasam.edu.br/wp-content/uploads/2016/06/Bitcoin-A-Moeda-na-Era-Digital.pdf.

https://pt-br.eventials.com/DaviTrindadeBatista/aula-1-apresentacao-do-curso-e-o-que-e-bitcoin.

https://www.tecmundo.com.br/bitcoin/51562-como-comprar-e-vender-bitcoins-no-brasil.htm.

https://www.infomoney.com.br/blogs/cambio/moeda-na-era-digital/post/5670719/volatilidade-bitcoin-tem-caido-ano-apos-ano.

https://www.criptomoedasfacil.com/as-5-principais-criptomoedas-alternativas-e-suas-diferencas/

https://portaldobitcoin.com/top-10-altcoins-tudo-o-que-voce-precisa-saber-sobre-concorrentes-bitcoin/

https://tecnoblog.net/141789/silk-road-ross-ulbricht-preso/

http://www.coachfinanceiro.com/portal/vantagens-e-desvantagens-em-usar-os-bitcoins-e-outras-moedas-virtuais-existentes/

https://atlasproj.com/blog/vantagens-moeda-digital-bitcoin/

https://atlasproj.com/blog/bitcoin-e-seguro/

https://www.tudocelular.com/curiosidade/noticias/n103620/Bitcoin-e-ambiente-por-que-as-criptomoedas-podem-ser-prejudiciais-a-natureza.html

https://medium.com/@markusbkoch/riscos-e-desvantagens-do-bitcoin-55967426ea7e