BLOCKCHAIN

Autores: Diego Rodrigues Brunoro, Gustavo Berté da Luz, João Vitor Kussler de Souza, Jonathan Igor Bockorny Pereira, Líndice Lopes Leonardi, Matthias Weber.

Instituição: Faculdade Dom Bosco Porto Alegre- RS.

Orientador: Filipo Novo Mór.

SUMÁRIO:

INTRODUÇÃO:

DEFINIÇÃO BLOCKCHAIN:

Blockchain pode ser definido como uma base de dados descentralizada, que guarda uma quantidade crescente de registros (blocos), cada um destes blocos contém um hash, uma Indicação de tempo, e os dados da transação. A blockchain foi feita para ser resistente à modificação de informação, como se fosse um livro-registro aberto que pode guardar transações entre duas partes de maneira eficiente, verificável e permanente.

HISTÓRIA

Blockchain teve sua origem do código fonte do Bitcoin em 2008 por Satoshi Nakamoto, que em 2009 liberou o código como código aberto. Assim iniciando a mineração de Bitcoin até os dias de hoje, a principio o código não foi muito bem aceito pela comunidade, desconfiavam do futuro do Bitcoin pois haviam tentativas parecidas anteriormente que não deram certo. O preço do bitcoin foi decidido no fórum BitcoinTalk, que também foi fundado por Satotshi. Em 2010 houve um único caso conhecido em que a Bitcoin foi adulterada, resultando em 184 bilhões de bitcoins em uma única transação mas foi corrigido em poucas horas após a descoberta. A partir de 2011 o código foi abandonado e a partir deste momento foi lentamente desenvolvido e minerado pela comunidade que também resolvia alguns erros que ainda haviam no código, e a partir de 2013 que as empresas começaram a aceitar bitcoins como forma de pagamento já que a criptomoeda não tinha taxas absurdas, o que tornou a moeda mais viável para trocas comerciais entre grandes empresas e investidores. A explosão de valor que ocorreu em 2017 ocorreu em resposta do grande movimento em torno do Bitcoin com vários países discutindo se aceitariam ou não a criptomoeda de forma oficial.

Outra moeda bem popular é o Ether, conhecida por ser a a geração Blockchain 2. 0, diferente de outas criptomoedas ela é usada exclusivamente na plataforma Ethereum, fundada por Vitalik Buterin como um código aberto desenvolvido em 2013 e liberado para os usuários em 2014 para testes com o nome de Frontier, junto com uma iniciação de levantamentos de fundos para o desenvolvimento, o Ether é usado como forma de pagamento pelo Gás dentro da plataforma Ethereum para executar ações, mas não precisa necessariamente ser paga em Ether, e em 2015 houve um engate quando sofreu um hack. Com a perda de quase U$60 milhões, a ferramenta apresentou vulnerabilidade, mas a solução para este problema foi retaliar os hackers, e com isso a moeda ganhou um aumento de valor e sofreu uma bifurcação, dando origem a duas outras tecnologias Ethereum Classic e Ethereum.

Uma criptomoeda que surgiu de uma piada, Dogecoin surgiu quando Billy Markus decidiu criar uma moeda virtual divertida para que atingisse um público maior, e ao modificar código do Bitcoin ele criou sua própria moeda, o Dogecoin mas isso não era o suficiente, mas após Jackson Palmer ser incentivado por um estudante no Twitter ele resolveu investir na moeda, assim dando valor ao Dogecoin. A princípio a moeda era utilizada como forma de dar gorjetas a outras pessoas, ela ganhou uma popularidade incrível nos fóruns e com isso seu recrescimento foi muito rápido. Atualmente a moeda perdeu muito do seu valor por conta da remoção do limite na produção de Dogecoin, tornando sua produção ilimitada e assim tornando-a em uma moeda inflacionária

CRIPTOGRAFIA:

Oriunda da junção das palavras gregas “Kryptos”(escondido, oculto) e “Gráphen”(escrita), a criptografia tem quatro objetivos, confidencialidade, integridade, autenticação e não repudio ou irretrabilidade.

Desde os primórdios da humanidade, a criptografia sempre esteve ao lado do homem como forma de esconder sua comunicação. Atualmente os exemplos mais famosos são a Assinatura Digital e o Blockchain, que utilizam o conceito de chave criptográfica.

A técnica mais conhecida na criptografia é a chave Criptográfica, caracterizada como conjunto de bits baseado em um determinado algoritmo matemático capaz de decodificar a informação podendo ser simétricas, de chave única, ou assimétricas, com chave pública e privada.

Na chave simétrica, tanto o emissor quanto o receptor usam a mesma chave para codificar e decodificar a mesma mensagem. Temos como exemplos os algoritmos DES(Data Encryption Standart) criado pela IBM em 1977, com chave de 56 bits, 72 quatriliões de combinações. O RC(Ron´s Code) criado por Ron Rivest, com chaves que vão de 8 a 1024 bits.

Na chave assimétrica existem as chaves publicas e privadas, onde a chave privada é usada para decifrar mensagens, enquanto a publica é utilizada para cifrar um conteúdo. Portanto quando precisarmos enviar um conteúdo para alguém, é necessário apenas a chave publica do seu destinatário, este usa a chave privada para decifrar a mensagem. Assim garantido a privacidade e maior confiabilidade de uma troca de dados. Uma das grandes aplicações da criptografia de chave assimétrica é a assinatura digital, utilizando-se de um hash e o algoritmo RSA.

O algoritmo que utiliza essa técnica é o RSA, registrada em 1977 no MIT, pelos cientistas da computação, Ronald Rivest e Adi Shamir, junto com a participação do matemático Leornard Adleman. O algoritmo era baseado na multiplicação de números primos de grande escala para a geração de uma chave pública. Assim dependendo do número, o tempo necessário para quebra da chave pode se tornar consideravelmente grande. Em 1999, no Instituto Nacional de Pesquisa da Holanda com trabalho de cientistas de 6 países e 300 computadores foram necessários 7 meses de trabalho para quebrar uma chave RSA com 512 bits.

Outra aplicação da chave assimétrica é o blockchain, que utiliza o algoritmo SHA-256, um conjunto de funções hash criptográficas pela NSA, oriunda da família SHA-2, o SHA-256 tem palavras computadorizadas de 32 bytes, quantidade de deslocamento e constante aditivas diferentes dos outros da mesma família

APLICAÇÕES DA BLOCKCHAIN

Aplicações não comerciais:

Desde sua criação o conceito de blockchain vem sendo associado a aplicações comerciais de compra e venda da criptomoeda conhecida por Bitcoin, porém sua aplicabilidade pode ser feita para diversas situações. As aplicações não comerciais mais utilizadas nos tempos atuais e que vem ganhando destaque são a criação de tokens de validação, onde são utilizadas tecnologias de criptografia avançada para protocolos de segurança dos tokens de confirmação e recentemente algumas instituições de ensino vêm utilizando as blockchains para validar certificados de conclusão de cursos a fim de evitar fraudes envolvendo a falsificação de certificados oficiais. Também é importante atribuir o uso de blockchains para o combate de ciber ataques, onde sua aplicação é feita de forma poderosa para a segurança das redes IoT, sua aplicação vem sendo desenvolvidas de forma escalar onde pode-se enxergar o caminho que as aplicações de blockchains para o IoT, visando o controle e verificação em tempo real de assinaturas e dados falsos a fim de encontrar falsificações e evita-las.

Aplicações comerciais:

O uso de blockchain para aplicações comerciais está cada vez maior, tendo seu uso principal em meios como serviços de telecomunicações e econômico, porém suas aplicações podem ser utilizadas muito além destes dois nichos. Entre eles pode-se observar o uso de forma diversificada bem como um recurso, algumas dessas aplicações que já foram aplicadas são:

BlockPoints – Essa tecnologia foi desenvolvida utilizando aplicações de blockchain para meios de pagamentos, onde é possível utilizar a carteira virtual, também foi desenvolvida para programas de fidelidade e cartões de presentes entre outros tipos de aplicações comerciais.

Warranteer – Essa aplicação permite acesso fácil a informações sobre produtos que foram adquiridos para obter assistência técnica em caso de mau funcionamento dos mesmos.

Guts – Este sistema que foi desenvolvido utilizando blockchain possibilita o usuário verificar se o ingresso adquirido é verdadeiro ou se é uma falsificação.

As aplicações envolvendo blockchain integrada a sistemas continua em evolução, onde pode-se perceber outras variações para seu uso, além do comum onde a blockchain é utilizada apenas para efetuar transações de criptomoedas. Outro tipo de aplicação muito utilizado para fins comerciais é dentro do ramo do varejo, onde já é possível efetuar pagamentos utilizando esse mecanismo de blocos como carteira virtual e transferindo as criptomoedas para os respectivos destinatários.

IMPLEMENTAÇÕES DA BLOCKCHAIN

Ao contrario do que todos pensão o conceito do blockchain, vai além das cripto moedas, o Blockchain que traduzindo para o português significa “cadeia de blocos” serve para dar validade a uma informação, fazendo com que todos os blocos estejam sempre alinhados, ou seja uma rede de compartilhamento de dados que se auto valida impedindo ou dificultando que ocorram fraudes, é muito comum ler resenhas na internet sobre Blockchain e bitcoin, pois de certa forma a forma de trabalho ficou mais popular desta forma no entando devemos nos atentar para o blockchain ser apenas umas das ferramentas utilizadas para que agregue valor ao negocio desejado.

Entre as possibilidades de aplicações do blockchain estão a criação de ativos (Moedas virtuais), aumento da segurança da informação, maior rastreabilidades das transações gerenciar desde Identidades até mesmo gerenciar uma cadeia de suprimentos inteiros como a logistica, unificar informações médicas entre outras inumeras aplicações, porem dev se levar em conta que somente o blockchain não é uma solução, por exemplo precimos adicionar outras ferramentas e softwares de acordo com as intenções de onde sera aplicado.

Claro que da mesma forma que o blockchain agrega essas amenidades ele também traz a extinção de alguns postos de trabalho como a conciliação de balancetes e contas bancarias uma vez que o proof of work realiza esta conciliação com assertividade de 100%, talvez até diminua a possibilidade de corrupção uma vez que é difícil ou até mesmo impossível esconder todos os rastros deixados através da cadeia de blocos obviamente dependendo da forma que foi aplicado.

Estima-se que uma pequena parte da população mundial conheça o conceito e aplicação do Blockchain, comumente confundindo com apenas aplicação em criptomoedas, é um conceito um pouco novo mas que tem o potencial de agregar bilhoes de dolares a empresas no mundo todo e que desejam aplicar esta tecnologia a seu favor.

LIMITAÇÕES DA BLOCKCHAIN

3 APLICAÇÕES QUE LEVAM VANTAGEM DA BLOCKCHAIN

Diante das transformações no mercado financeiro nos últimos anos, as empresas estão voltando seu olhar a operações que utilizam da tecnologia do blockchain pela transparência nas transações que são todas Open Source(código aberto) para que qualquer usuário possa acessar e ver como acontece as transações entre usuários. Algumas aplicações que levam vantagens na Blockchain:

3.1 CRIAÇÃO DE MARKETPLACES

O uso de Blockchain dispensa supervisão de terceiros entre as transações fazendo com que sejam totalmente seguro uma vez que os usuários tem as permissões necessárias para corrigir possíveis erros e auditar. Diante disso as ações de compra e venda se tornam mais simplificadas e rápidas, os usuários estarão menos sujeitos a possíveis golpes e fraudes de produtos comprados pela internet, por isso o crescimento dos marketplace é um atrativo ao uso de blockchain que consegue realizar essas transações de forma segura para ambos lados.

3.2 GERENCIAR REGISTROS PRIVADOS DESCENTRALIZADOS

Apesar de toda tecnologia que temos atualmente, guardar dados pessoais ainda é um assunto sensível quando falamos em banco de dados, muitos bancos de dados tem suas fragilidades e já relatamos diversas empresas de grande porte ter seus dados roubados por hackers. O que a utilização da Blockchain sanaria pois cada dado é guardado de forma criptografada dentro dos blocos, para acessar é preciso desbloquear diversas chaves que utilizam da criptografia para manter e assegurar a integridade de seus dados, o que também evitaria roubo de dados e falsificação de documentos.

4 APLICAÇÕES QUE NÃO LEVAM VANTAGEM NA BLOCKCHAIN

Assim como toda nova tecnologia, o Blockchain não ficaria por fora no quesito de desvantagens, já que algumas aplicações ainda não estão definitivas, muitos usuários ainda encontram dificuldades em lidar com as transações ou pensam a longo prazo até quando essa tecnologia será utilizada e se vão perder alguma coisa ou não. Algumas aplicações que não levam vantagens na Blockchain:

4.1 MINERAÇÃO

Uma prática muito utilizada no mundo da Blockchain é a mineração, usuários que se dispõem em examinar os blocos e verificar possíveis fraudes durante a transferências entre carteiras de usuários. Porém, o processo de mineração exige um gasto excessivo de energia já que é necessário ter uma máquina ligada todo tempo para verificar diversos blocos simultaneamente, o que limita um pouco o uso da tecnologia.

4.1 IMUTÁVEIS SMART CONTRACTS

Uma vez que um smart contract é adicionado a rede da Blockchain ele se torna imutável pois não pode mais ser alterado, isso vem se tornando uma preocupação aos usuários que possuem

muitas moedas virtuais, pode vir a ser facilmente invadida por hackers. Como a blockchain é imutável estas ações são muito difíceis de serem refeitas o que pode ocasionar uma grande perda de valores nas carteiras dos usuários que não realizarem um smart contract bem sucedido.

CONCLUSÃO:

Os alunos do curso de iniciação cientifica da faculdade Dom Bosco juntos com o prof. Filipo Novo Mór, atraídos pela novidade da Blockchain e suas aplicações, fizeram uma pesquisa aprofundada sobre o tema com o proposito de compartilhar os conhecimentos da blockchain, dado que atualmente não a um fácil acesso a conteúdos relacionados ao tema.

REFERÊNCIAS

https://blogbrasil.comstor.com/como-implementar-a-tecnologia-blockchain-nos-negocios

https://www.grantthornton.com.br/insights/articles-and-publications/especial-blockchain/como-sua-empresa-pode-implementar-o-blockchain/

PFÜTZENREUTER, Elvis. Quais são as vantagens e desafios do Blockchain? 2018. Disponível em: <http://minerando.com.br/quais-sao-as-vantagens-e-desafios-do-blockchain/>. Acesso em: 10 set. 2018.

PRADO, Jean. O que é blockchain: indo além do bitcoin. 2018. Disponível em: <https://tecnoblog.net/227293/como-funciona-blockchain-bitcoin/>. Acesso em: 10 set. 2018

FAUVEL, Warren. Blockchain Advantage and Disadvantages. 2018. Disponível em: <https://medium.com/nudjed/blockchain-advantage-and-disadvantages-e76dfde3bbc0>. Acesso em: 10 set. 2018.

https://livecoins.com.br/historia-do-bitcoin/

http://www.historiadetudo.com/historia-do-bitcoin

https://www.criptonario.com.br/historia-do-ethereum/

https://cryptodaily.co.uk/the-history-of-ethereum/

https://www.investinblockchain.com/what-is-dogecoin/