**CENTRO UNIVERSITÁRIO DE ITAPIRA**

**ESTRUTURA DE DADOS EM BLOCKCHAINS**

**DARA STRUCTURE IN BLOCKCHAINS**

Gabriel Martins de Almeida

Marco Antônio Ferreira Filho

**RESUMO**

O Blockchain é uma tecnologia que consiste em um banco de dados distribuído, online e público. São implementadas técnicas de criptografia para que cada participante possa manipular o ledger de forma segura e sem a necessidade de uma autoridade central criando um registro que é compartilhado e protegido. Uma vez que um bloco é adicionado, é extremamente difícil alterar ou remover. Até agora, o blockchain tem atraído bastante atenção da indústria de serviços financeiros, mas a tecnologia pode ser adaptada para qualquer indústria onde seja necessário registrar, confirmar e transferir qualquer tipo de contrato e oferecendo ao mesmo tempo um alto nível de segurança. Atualmente, existem apenas pequenas iniciativas e, por enquanto, ainda não está claro seu limite de alcance em relação as suas funcinalidades no future ao seu futuro. A Tecnologia foi apresentada em 2008 por Satoshi Nakamoto, e foi um grande marco para a criação do bitcoin.

**Palavras-Chave**: Blockchain, Criptografia, Banco de Dados, Estrutura de Dados.

**ABSTRACT**

Blockchain is a technology that consists of a distributed, online and public database. Encryption techniques are implemented so that each participant can handle the ledger safely and without the need for a central authority creating a record that is shared and protected. Once a block is added, it is extremely difficult to change or remove, the concept was introduced in 2008 by Satoshi Nakamoto. So far, blockchain has attracted a lot of attention from the financial services industry, but the technology can be adapted to any industry where it is necessary to register, confirm and transfer any type of contract while offering a high level of security. Currently, there are only small initiatives and, for now, several aspects related to its future are not yet clear.

**Keywords**: Blockchain, Cryptography, Database, Data Structure

**1 INTRODUÇÃO**

Com o aumento dos ataques cibernéticos, a segurança de dados que circulam o mundo virtual através de transferências digitais é cada dia mais importantes, e o Blockchain uma estrutura de dados distribuída que surgiu em 2008 com mecanismos diferentes dos já conhecidos tomando fama atuação na área dos Bitcoins onde ele emprega um registro público anônimo onde todos podem participar mantendo total sigilo de identidade. Além de distribuído, outra característica que da um destaque a mais a tecnologia e sua descentralização, ou seja, não existe uma unidade central que controla os dados, o sistema funciona como uma fila em blocos que liga o dado anterior ao próximo formando um tipo de fila. O grande marco da Blockchain em relação a sua segurança está justamente na ligação destes blocos, podemos imaginar uma grande fila interligada de transação de grandes valores comerciais, portanto a segurança consiste em que se houver alguma tentativa de ataque com o objetivo de modificar a transação obrigatoriamente terá que ser modificado mais da metade da rede. Vale ressaltar que nem tudo são flores como comenta alguns estudiosos sobre o alto consumo de Processamento necessário para suportar uma estrutura como essa.

“Um dos problemas encontrados na prova de trabalho (proof of work) é o custo energético, a produção de vários hashes até encontrar um válido, há um alto consumo de energia para os processadores ASIC’s (hardware específico para mineração) conseguirem encontrar o próximo hash válido para o bloco. Por conta disto, está se discutindo uma nova forma de mineração, chamada de proof of stake ou prova de participação. Dentre os pontos positivos de utilizar blockchain tem-se o baixo custo, seguro, sem intermediários, imutável, único, público e com facilidade de transações internacionais.” (ALIAGA; HENRIQUES, 2017)

Esses Pontos serão abordados mais profundamente, destrinchando e analisando pontos específicos e falhas da estrutura que mostra ainda hoje grande capacidade de segurança quando falamos de arquivamento de documentos com registro e assinatura digital.

**2 METODOLOGIA**

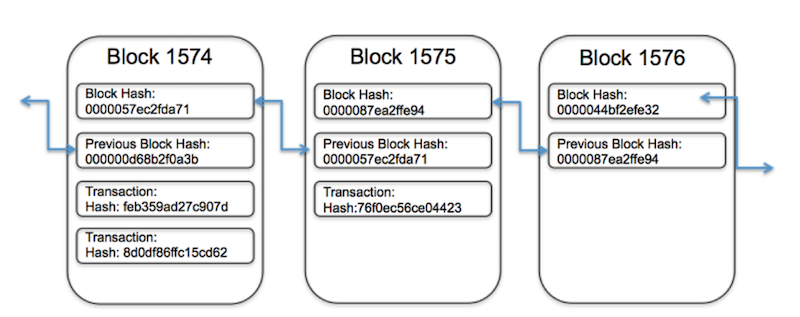
A consolidação do desenvolvimento em prol da conclusão do trabalho, que consistem na análise da aplicação e implementação blockchain para o intuito de arquivamento e proteção de registros em estruturas de dados complexas e simples, foi realizada por meio de pesquisas em base de estudos já realizados, buscados em artigos semelhantes, livros e com auxílio da internet, os dados da segunda etapa formaram-se pela análise dos estudos semelhantes validando e complementando questões relacionadas ao texto e seus fundamentos.

**3 RESULTADOS**

Os resultados obtidos trabalham em conjunto com as teses de construção de uma estrutura em blockchain e a apresentação da tecnologia para o público desinformado. Porém obteve-se um conjunto de sugestões de aplicações do blockchain, destaques de falhas do sistema, e produtividade no mercado administrativo bem como segurança provida em armazenamento de transações virtuais.

**3.1 Características do blockchain**

Buscando conhecer o funcionamento e os principais fatores que fazem do blockchain uma das tecnologias inovadoras, através dos estudos selecionados, as suas principais características. Ele é como uma cadeia ordenada de blocos protegidos por um processo de resolução de um resultado de trabalho PoW. O entrelaço é feito adicionando o hash de um bloco anterior ao bloco atual. Os blocos aninhados consecutivos garantem que as transações sejam enviadas em ordem respectivamente relacionada ao tempo que foram solicitadas, portanto, uma transação não pode ser alterada com antecedência sem alterar junto todos os blocos a seguir. Assim podemos afirmar que o blockchain torna inviável o ataque de duplicação de gasto, a menos que o invasor controle mais de 51% do poder computacional da rede inteira o que é extremamente improvável.



**Fonte**: <https://celere-ce.com.br/inovacao/blockchain-no-mercado-de-construcao/>

**3.2 Blockhain e o bitcoin**

Infelizmente, ou felizmente, não temos como falar de blockchain sem tocar no assunto de bitcoin, pois foi graças a está ideia primordial que surgiu a moeda virtual mais importante e uma das, senão a mais valiosa do mundo moderno. No livro “BITCOIN – A Moeda Na Era Digital” de Fernando Ulrich que nos conta um pouco mais dilacerando partes da história e nos mostrando desde a sua invenção ate seu auge na modernidade:

“Bitcoin é como um grande livro-razão, único e compartilhado por todos os usuários simultaneamente. Nele, todas as transações são registradas, sendo verificadas e validadas por usuários especializados, de modo a evitar o gasto duplo e que usuários gastem saldos que não possuem ou de terceiros. Esse registro público universal e único não pode ser forjado. Lá estão devidamente protocoladas todas as transações já realizadas na história do Bitcoin, bem como os saldos atualizados de cada usuário. O livro-razão é, assim, um registro fidedigno, estando sempre atualizado e conciliado. Por sinal, o nome dado a esse livro-razão é blockchain.”

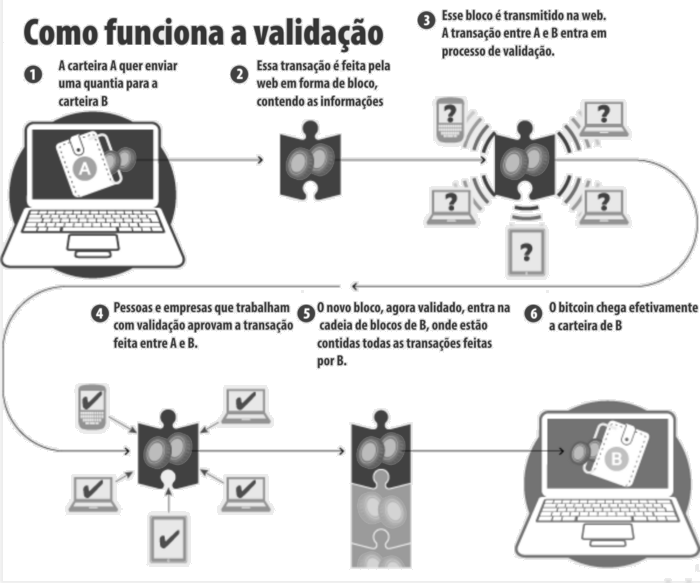
(ULRICH; FERNANDO, 2014, p.112).

Destaca-se Também no livro a maneira como foi dada importância a criptografia na era digital e os pontos que possibilitaram a criação do bitcoin.

“Mas para entendermos melhor como a ciência da computação e a internet possibilitaram a criação do experimento Bitcoin, é preciso ir mais além e compreender as principais tecnologias intrínsecas ao sistema. Basicamente, o Bitcoin é a junção de duas tecnologias: a distribuição de um banco de dados por meio de uma rede peer-to-peer e a criptografia. A primeira foi somente possível com o advento da internet. Já a segunda é bastante antiga, mas seu potencial não poderia ter sido devidamente explorado antes da era da computação. Ao contrário das redes usuais, em que há um servidor central e os computadores (clientes ou nós, nodes, em inglês) se conectam a ele, uma rede peer-to-peer não possui um servidor centralizado. Nessa arquitetura de redes, cada um dos pontos ou nós da rede funcionamos tanto como cliente quanto como servidor – cada um dos nós é igual aos demais (peer traduz-se como “par” ou “igual”) –, o que permite o compartilhamento de dados sem a necessidade de um servidor central. Por esse motivo, uma rede peer-to-peer é considerada descentralizada, em que a força computacional é distribuída.

(ULRICH; FERNANDO, 2014, p.44).

Com tais citações de Ulrich podemos ver claramente o ponto em que a grande inovação aconteceu onde a rede deixou de ser centralizada e passou a ser entrelaçada entre blocos internos difundindo as informações e criando laços, como e possível ver na imagem abaixo desde a efetuação da transação ate a adição de um novo bloco mostrando como funciona a validação com segurança dentro da rede.



**Fonte**:<https://medium.com/@chorarthur/bitcoin-pequeno-dicion%C3%A1rio-a0a72cf890bb>

**3.3 Programação do Blockchain**

O imperador por trás do bitcoin foi inicialmente desenvolvido em c++ e embora sua aplicação na linguagem já esteja datada ainda há quem utilize. Essa técnica hoje pode ser aplicada nas mais diversas linguagens de programação respeitando suas sintaxes e são oferecidos muitos cursos gratuitos e pagos para quem se interessa ao aprendizado. Em um estudo dirigido por Fernando Américo (estudante de economia e entusiasta de criptomoedas e mundo tecnológico como um todo. Trabalha em vários portais pessoais e de terceiros como redator e editor web.), que adaptou o texto do site “makeeuseof” o mesmo deixa claro a facilidade da aprendizagem:

“Se você é um desenvolvedor de software e já possui todas as habilidades de programação básica descritas acima, você pode mergulhar direto no aprendizado da programação blockchain hoje. Os recursos a seguir fornecem plataformas e ambientes on-line para ajudá-lo a praticar o desenvolvimento de seus próprios aplicativos blockchain. [...] Programação Blockchain não é um conceito simples por qualquer trecho da imaginação. No entanto, se você já é um programador, então você tem a base necessária para aprender programação blockchain.” (AMÉRICO; FERNANDO, 2019, 99cripto).

Voltando a atenção para a parte mais pratica e menos teórica, podemos pensar e uma construção de um bloco simples.

[

“remetente” =>” mario”,

“destinatário” =>” jose”,

“mensagem” =>”0.1 BTC”

]

Um estrutura em php para construir um bloco simples, porem o grande segredo esta na ligação do bloco com o restante da fila de processos e seu entrelaçamento, vejamos agora um exemplo de uma função para ligar o bloco ao corrente, passando por parâmetro a função um bloco novo, pegando o blockchain que está na memoria e primeiramente verificando se está vazia ou não criando um primeiro bloco que nada mais é que um bloco dele mesmo para dar início a sequência.

Function adiciopnalbloco($bloco\_novo) {

If ($blockchain – array ()) {

$bloco\_novo[“hash”] = hash (“sha256”, json\_encode($bloco\_novo));

} else {

$ultimo\_bloco = end($blockchain);

$bloco\_novo[“hash”] = $ultimo\_bloco[“hash”];

$bloco\_novo[“hash”] = hash (“sha256”, json\_encode($bloco\_novo));

}

Array\_push ($blockchain, $bloco\_novo);

}

}

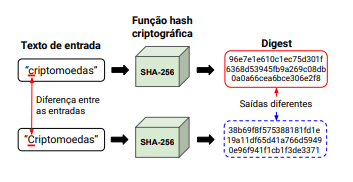
adicionaBloco($bloco\_1);

adicionaBloco($bloco\_2);

adicionaBloco($bloco\_3);

adicionaBloco($bloco\_4);

Com a inserção manual podemos realizar um método pra imprimir e terminamos um resultado básico de uma blockchain, criando uma base com bem mais ados o resultado seria o seguinte, ao mudar um elemento da mensagem “mensagem” =>”0.1 BTC”, como por exemplo colocarmos o valor 0.2 ao invés de 0,1, automaticamente mudaria o hash da transação de todas as transações anteriores, tornando o array entrelaçado com o hash ligado um a um

****

**Figura**: Aplicação de uma função hash criptográ­fica

**4 DISCUÇÃO**

Percorridas as etapas metodológicas propostas, foram apresentadas as principais características do Blockchain, suas aplicações e possibilidades; tratou-se, também, de conceituar a comunicação científica, identificar sua estrutura, suas etapas e seu suporte tecnológico. Nesta seção, pretende-se estabelecer de modo mais evidente a relação entre Blockchain e comunicação científica, identificando possibilidades de uso.

Constatou-se que o Blockchain, como mencionado anteriormente, é um sistema que possui como características essenciais a imutabilidade das informações, que são contidas de modo descentralizado, e sem a necessidade de um agente intermediador entre o serviço e o usuário. Basicamente esses três traços são as grandes inovações trazidas por essa tecnologia; logo, é possível percebê-los nas aplicações desenvolvidas com base no Blockchain. Exemplo disso, é o uso da Bitcoin, que tem todas transações guardadas de modo imutável, descentralizado (garantindo aspectos comprobatórios quanto às transações realizadas) e sem a necessidade de um banco com a função intermediador, já que tudo é realizado pelo próprio sistema.

Contudo, ainda não se deve desconsiderar as outras propriedades, como a atualidade, irrefutabilidade, prevenção contra duplicação, transparência – para citar as principais. Todos esses atributos fazem da tecnologia o que ela é, e como visto nas suas aplicações, eles são mais ou menos explorados dependendo da proposta e necessidade do sistema desenvolvido. É o que acontece, por exemplo, com a transparência: o sistema pode ou não ser desenvolvido para permitir a adição, validação e visualização somente por pessoas autorizadas, por meio de um Blockchain privado.

Se, de um lado, é possível desenvolver um sistema que use Blockchain privado, e que não fique acessível a qualquer pessoa (é possível restringir a transparência àqueles autorizados), de outro, há atributos dessa tecnologia que não podem ser abandonados, como ocorre no caso da imutabilidade. Essas características estão presentes na própria ideia e estrutura do Blockchain, mas, mesmo assim, de modo geral, nem todos os usos dessa tecnologia se beneficiam explicitamente de todas essas características.

Dependendo do uso que se faz, atributos diferentes transparecem como propriedades indispensáveis naquele determinado contexto. Exemplos ajudam a deixar isso claro. Um deles é o uso do Blockchain aplicado à cadeia de suprimentos: a tecnologia como ferramenta empregada no processo que vai do planejamento ao consumo de alimentos. Nesse caso, são explorados principalmente a imutabilidade e atualidade dos dados, ainda que as outras propriedades também estejam presentes dando suporte a esse funcionamento.

Nesse tipo de sistema é fundamental entregar ao consumidor uma informação íntegra, ou seja, inalterada; quanto à atualidade, é imprescindível que tais informações correspondam fielmente ao tempo em que o correspondente processo foi realizado, pois isso influi tanto na venda desse produto – ao se pensar que um produto fresco e preservado em condições ideais tem mais demanda por parte dos revendedores – e também na escolha dos consumidores, que logicamente, ao saber que esse produto foi colhido, abatido ou processado em uma data, horário ou condições especificas, também dão preferencia a eles. A atualidade se mostra útil também ao se pensar em um serviço realizado por etapas.

A informação rápida sobre o processo permite planejamento e antecipação. Possibilita prever, em fases posteriores, a chegada do produto, o que é vantajoso principalmente para a identificação de problemas e tomada de decisão, adoção de medidas para lidar com a situação. Além disso, o acesso a essas informações, como um todo, também constitui um fator diferencial, pois permite ao consumidor, por meio de um código, como o de barras, acessar toda a trajetória do produto, tornando o serviço prestado transparente e confiável. Em tempos em que consumidores se preocupam e buscam, cada vez mais, informações sobre o que compram, isso parece uma característica desejável.

É importante deixar claro que pensar nos usos do Blockchain não implica, necessariamente, em abandonar as práticas e suportes usualmente empregados. Nesse sentido, pode-se observar esses sistemas de outro modo: a partir da possibilidade de mesclar diversas outras tecnologias já atualmente utilizadas, o que reforça que o Blockchain não veio para substituí-las, obrigatoriamente, mas sim aperfeiçoá-las em aspectos anteriormente não possíveis. É o que ocorre nos sistemas Pluto e Scienceroot, desenvolvidos para finalidades científicas.

Ambos os sistemas se apoiam na tecnologia Blockchain, mas adotam banco de dados que assume serviços ainda não viáveis, de modo satisfatório, em um Blockchain: a inserção de arquivos. Por possuírem um tamanho muito maior do que o que se tem em uma simples transação de valores de criptomoedas, um Blockchain para troca de arquivos impediria o sistema de funcionar com agilidade, vista a necessidade de se resumir, distribuir e validar todos esses arquivos dentro do sistema. Nesse caso, como ocorre no Scienceroot, todos os arquivos estão guardados em um sistema de armazenamento P2P chamado InterPlanetary File System (IPFS), que tem a função de guardar e atribuir um endereço ao arquivo. Sendo assim, o que é registrado em uma transação de Blockchain não é o arquivo, mas os links IPFS referentes a eles. Isso mostra a imutabilidade sendo adaptada e utilizada concomitantemente a outras tecnologias, criando um serviço não visto até então com o uso na Bitcoin.

Vale ressaltar que o IPFS possui mecanismos próprios de garantir a integridade das informações, como o uso de hash criptográfico nos arquivos armazenados, garantindo que o sistema por completo, e não só a camada de Blockchain, seja seguro (GÜNTHER e CHIRITA , 2018). Mas, como dito, esses sistemas fazem mais do que uma simples guarda de arquivo. No Scienceroot, há uma plataforma colaborativa em que os autores se cadastram e a partir de então têm a possibilidade de usufruir do sistema de forma gratuita. Esse sistema permite ao pesquisador se conectar com diversos outros pesquisadores, colegas e com os pares do seu campo de pesquisa, podendo compartilhar dados ou até a própria pesquisa.

Por ter entre suas propostas a publicação de pesquisas e apesar de se saber que há a presença dos pares, não é claro como essa avaliação ocorre ao se ler os documentos referentes a plataforma. Há ainda a presença de uma moeda própria: Science token, utilizada como recompensa para validadores e, além disso, permite que pesquisadores arrecadem fundos para sua investigação por meio de doação de outros usuários. Também há a oportunidade de fazer perguntas, respondê-las e achar soluções para o problema da pesquisa, além de outras funcionalidades (GÜNTHER; CHIRITA, 2018).

Desenvolvida para ser uma rede de pesquisa, a plataforma Pluto lida com as trocas de valor realizadas em todo o ciclo da pesquisa, sendo entendido como valor desde uma troca de informação a quantias monetárias. Esse sistema não restringe o tipo de publicação, exigindo somente que a informação publicada tenha “[...] o 79 potencial de agregar valor à progressão científica, incluindo, mas não se limitando a propostas, ideias de pesquisa, hipóteses, projeto de experimentos, protocolos de pesquisa, dados experimentais, análises e interpretações” (PLUTO, 2018, p. 16, tradução nossa).

As licenças dos seus trabalhos ficam sob total controle dos próprios pesquisadores, e os direitos autorais de sua obra também são definidos por eles, diante de diversas opções já dadas pelo sistema. A revisão por pares segue parecida, em partes, com o modelo tradicional. Todos podem avaliar, porém há a exigência de uma comprovação de reputação. Ao se submeter um documento, inicia-se a revisão às cegas, em que o avaliador obrigatoriamente deve incluir comentários detalhados sobre o que foi avaliado. Além de aceitar e recusar, o avaliador ainda tem a opção de pedir a revisão do documento, que, ao ser realizada, retorna ao avaliador e assim, definitivamente, aprova ou recusa. Por fim,

48 horas após a revisão por pares ou o envio da versão revisada, tem-se o fim da revisão as cegas e ambos, autores e avaliadores, têm sua identidade revelada (PLUTO, 2018).

**3 CONSIDERAÇÕES FINAIS**

Tendo como base nossos estudos, constatamos que o blockchain trouxe soluções novas para antigos problemas. Um paradigma aberto, descentralizador, e acessível dá-nos a entender que os dados contidos em seus blocos de comando sejam de alta confiança, com grande importância no registro de transações, rastreabilidade e comprovação de propriedade, mesmo ainda tendo muito a se desenvolver o que nos dá um pensamento positivo a respeito do seu futuro. Embora seja recente no mundo da tecnologia, atualmente no ano de 2020 ele já se encontra bem difundido e avançado em relação aos anos posteriores, principalmente em meados de 2008 onde aparecia como uma tecnologia imatura para substituir soluções tradicionais da época, hoje esse tipo de estrutura já é cotada para uso em grandes organizações, devido a prova de sua eficiência. E obviamente não deixemos de destacar suas desvantagens, entendemos que o blockchain é uma solução que revolucionou a década e que cada dia atrai a atenção de desenvolvedores e empresas, portanto, seus defeitos são propícios a serem corrigidos à medida que sua utilização se tornar mais difundida pelo mundo, hoje, grande parte dos problemas apresentados a anos atrás já foram amenizados, tornando o uso do sistema muito mais viável.

**REFERÊNCIAS BIBLIOGRÁFICAS**

* ALBAGLI, Sarita. Divulgação científica: informação científica para a cidadania?. Ciência da Informação, Brasília, v. 25, n. 3, p. 396-404, dez. 1996. Disponível em: . Acesso em: maio. 2018.
* Blockchain: Blueprint for a New Economy – Melanie Swan
* Bitcoin: A Moeda na Era Digital – Fernando Ulrich
* A Revolução das Moedas Digitais. Bitcoins e Altcoins – Tatiana Casseb B. M. Barbosa
* ANTONOPOULOS, Andreas M. Mastering bitcoin: unlocking digital cryptocurrencies. Sebastopol: O’Reilly, 2014. 282 p.
* CENTRO DE PESQUISA E DESENVOLVIMENTO EM TELECOMUNICAÇÕES (CPQD). Blockchain: uma visão geral. Campinas: CPQD, [2017?]. 30 p. Disponível em: . Acesso em: abr. 2018.
* GIL, Antônio Carlos. Como elaborar projetos de pesquisa. 4. ed. São Paulo: Atlas, 2002.
* G1. Mundo tem 3,2 bilhões de pessoas conectadas à internet, diz UIT. Disponível em: . Acesso em: abr. 2018.
* LIEVROUW, L. A. Communication and the social representation of scientific knowledge. Critical Studies in Mass Communication, Annandale, v. 7, n. 1, p. 1- 10, Mar. 1990.
* NAKAMOTO, Satoshi. Bitcoin: A Peer-to-Peer Eletronic Cash System. 2008. 9 p. Disponivel em: . Acesso em: fev. 2018.
* SAP. Blockchain e tecnologia de banco de dados distribuído. 2018. Disponível em: . Acesso em: abr. 2018.