Origens da Blockchain: relato das tecnologias subjacentes às criptomoedas

Blockchain Origins: an account of the technologies underlying cryptocurrencies

DOI:10.34115/basrv7n2-004

Recebimento dos originais: 25/04/2023
Aceitação para publicação: 27/05/2023

Ronaldo Borges do Val
Doutorando em Ciência da Informação pela Universidade Fernando Pessoa (UFP)
Instituição: Universidade Fernando Pessoa (UFP)
Endereço: Praça 9 de Abril, 349, 4249-004, Porto-Portugal
E-mail: ronaldobval@gmail.com

Luis Borges Gouveia
Doutor em Ciência da Computação pela Universidade de Lancaster
Instituição: Universidade Fernando Pessoa (UFP)
Endereço: Praça 9 de Abril, 349, 4249-004 Porto-Portugal
E-mail: lmbg@upf.edu.br

RESUMO
O processo evolutivo da tecnologia Blockchain, tem sua origem a arquitetura elementos referenciados na Teoria de Sistemas Distribuídos e a integração diferentes tecnologias, incorporando características como a independência e simultaneidade de seus componentes, que coordenam ações de forma autônoma sem a presença de um elemento central, acrescentado no encapsulamento do software, sofisticados algoritmos matemáticos que definem as regras do negócio e a segurança dos dados, em contraposto aos sistemas tradicionais de acesso a um elemento central, suscetíveis a falhas, com controle limitado ou inexistente sobre os dados armazenados dos usuários, que possibilitam riscos de alterações ou exclusões de dados, sem que se tenha rastreabilidade garantida. Dentre as tecnologias incorporadas citamos as *Tecnologias de Registros Distribuídos, Estrutura de blocos, Criptografia de chaves assimétricas, função Hash, Assinatura Digital, Árvore de Merkle, Infraestrutura de Chaves Públicas, Escalabilidade, Mecanismos de Consensos, Contratos Inteligentes*, entre outras. A integração dessas tecnologias subsidiaram *Nakamoto(2008)* a criar a criptomoeda Bitcoin, o mais importante ecossistema de inovação baseado na Blockchain, que visava democratizar a moeda após a crise financeira de 2008, que desde então tem influenciado o surgimento de diferentes aplicações e inúmeros casos de uso.

Palavras-chave: tecnologias da informação, Blockchain, origens do Blockchain.

ABSTRACT
The evolutionary process of Blockchain technology, has its origin in the architecture of elements referenced in the Theory of Distributed Systems and the integration of different technologies, incorporating characteristics such as the independence and simultaneity of its components, which coordinate actions autonomously without the presence of a central element, added in the software encapsulation, sophisticated mathematical algorithms that

define business rules and data security, as opposed to traditional systems of access to a central element, susceptible to failures, with limited or non-existent control over the users' stored data, which allow risks of changes or deletions of data, without guaranteeing traceability. Among the incorporated technologies, we mention Distributed Registry Technologies, Block Structure, Asymmetric Key Cryptography, Hash Function, Digital Signature, Merkle Tree, Public Key Infrastructure, Scalability, Consensus Mechanisms, Smart Contracts, among others. The integration of these technologies supported *Nakamoto, S.(2008)* to create the Bitcoin cryptocurrency, the most important Blockchain-based innovation ecosystem, which aimed to democratize the currency after the 2008 financial crisis, which has since influenced the emergence of different applications and numerous use cases.

Keywords: Blockchain, technologies, origins.

1 INTRODUÇÃO

A contribuição de diferentes tecnologias que formaram a cadeia de blocos tem como referência o modelo de sistema de cofre de David Chaum (1982), que deram origem às cadeias de blocos em que descreve o projeto de um sistema de computador distribuído que pode ser estabelecido, mantido e confiável por grupos mutuamente suspeitos. A ideia de encadear blocos de informação imutavelmente com uma função hash criptográfica aparece na dissertação de 1979 de Ralph Merkle (1979) em Stanford, na qual Merkle explica como as informações podem ser vinculadas em uma estrutura de árvore agora conhecida como árvore hash Merkle (1982) e que posteriormente, em 1990, Stuart e Stornetta (1990) aplicaram essas ideias comparando a documentos com carimbo de data e hora, "*How to time-stamp a digital document in Advances in Cryptology: Proceedings of Crypto `90*" que descreveu a imutabilidade dos registros digitais com um Time Stamping Service (TSS) que usa funções de hash e assinaturas digitais para verificar a originalidade de um documento específico. Os documentos são encadeados para gerar uma sequência de tempo para verificar os carimbos de data/hora associados a cada documento. Essa cadeia de documentos com uma sequência de tempo foi a versão mais simples da Blockchain. A soma desses trabalhos subsidiaram Nakamoto (2008) a criar a criptomoeda Bitcoin, a primeira grande inovação da tecnologia Blockchain, que visava democratizar a moeda após a crise financeira de 2008, desde então tem influenciado o surgimento de diferentes aplicações em inúmeros casos de uso.

2 FUNDAMENTAÇÃO TEÓRICA

Partindo-se dos fundamentos de Sistemas Distribuídos, como base da tecnologia de Blockchain, sua arquitetura e os desafios em sua implementação compõem uma visão diferente de sua origem, muito além das criptomoedas. Estudos de casos e ecossistemas baseado na cadeia de blocos e uma breve explanação sobre as criptomoedas, em especial a comparação entre as duas principais Bitcoin e Ethereum formam a base para melhor entendimento a respeito das tecnologias subjacentes às criptomoedas que integradas montaram o que conhecemos hoje sobre a Blockchain.

3 SISTEMAS DISTRIBUÍDOS E A CADEIA DE BLOCOS DENOMINADA DE BLOCKCHAIN

Os Sistemas Distribuídos (SD) tem sua origem nas arquiteturas de sistemas operacionais estudadas na década de 1960. A ARPANET, a antecessora da Internet, foi introduzida no final da década de 1960 e o email da ARPANET foi inventado no início da década de 1970. O e-mail tornou-se a aplicação mais bem-sucedida da ARPANET e é provavelmente o primeiro exemplo de aplicação distribuída em larga escala. Logo na década de 1970, foram implementadas as redes locais, como a Ethernet. Diferentes esforços foram realizados para o desenvolvimento dos SD até sua evolução para as tecnologias da informação e da comunicação de dados, permitindo que componentes localizados em diferentes dispositivos em rede, se comuniquem, coordenem suas ações e interajam entre si visando alcançarem objetivos comuns.

4 REPLICAÇÃO DA MÁQUINA DE ESTADO

Várias arquiteturas de hardware e software são utilizadas pela computação distribuída, em um nível inferior visando conectar várias CPU em rede, em um nível superior e interconectar processos em execução nessas CPU com algum tipo de sistema de comunicação. Suas aplicações inicialmente ligadas às redes de telecomunicações, redes telefônicas e redes celulares evoluíram para as redes de computadores com a chegada World Wide Web e das redes ponto a ponto como aplicações de jogos online, comunidades de realidade virtual, aos negócios na utilização para as corporações e o meio científico. O uso de sistemas de gerenciamento de banco de dados distribuídos, adotando o processamento de informações distribuídas aplica-se aos sistemas bancários, sistemas de reservas de companhias aéreas e controle de processos em tempo real entre outras diversas aplicações. Majeed, et al (2021) citam que a computação distribuída, o estado e

a funcionalidade do sistema são replicados em toda a rede para fornecer serviços tolerantes a falhas bizantinas e sustentabilidade em caso de falha de alguns nós. Cada nó da rede mantém o mesmo estado determinístico de modo que, apesar da falha de algum nó, o estado do sistema permanece disponível (Nogueira; Casimiro e Bessani, 2017).

5 TEORIA DOS SISTEMAS DISTRIBUÍDOS

Um sistema distribuído é aquele no qual os componentes localizados estão localizados em diferentes dispositivos interligados em rede, comunicando-se e coordenam suas ações apenas passando mensagens conforme cita Coulouris; Dollimore e Kindberg (2007). Os sistemas distribuídos foram inicialmente propostos para o compartilhamento de recursos de componentes computacionais, a lista destes recursos foi amplamente estendida ao longo do tempo para diferentes tipos, controlados por diferentes ambientes operacionais e conectados em diversos tipos de redes. Requer um conjunto de funcionalidades e padronizações atuando entre a aplicação e o ambiente operacional, oferecendo uma abstração para a comunicação e representação dos dados, permitindo que diferentes aplicações executem em diversas plataformas, comunicando-se de forma transparente. A segurança é uma das propriedades que mais causa preocupações, o compartilhamento de recursos faz com que estes sejam visíveis a outros usuários do sistema, no entanto, eles devem ser protegidos de acessos indevidos. Mecanismos de privilégios de usuário, criptografia e tratamento de falhas são os elementos utilizados para garantir a segurança. Múltiplas requisições ou múltiplos acessos são realizados ao mesmo recurso e no mesmo instante de tempo. A implementação garante que todos os acessos e requisições sejam respondidos, garantindo acesso aos recursos do sistema, como se fossem locais.

6 TECNOLOGIA DE BLOCKCHAIN

Com potencial de gerar novas soluções tecnológicas ao mercado comparado ao modelo de aplicativos tradicionais, suas características como: confiabilidade, imutabilidade e auditabilidade de seus dados tornam-se um diferencial aos sistemas habituais. Elimina intermediários confiáveis em um processo transacional como o exigente nos sistemas centralizados tradicionais, por registrar as transações em um livro-razão distribuído, através de uma corrente de blocos, o processo dispensa a participação de terceiros na autenticação das transações, utilizando criptografias baseadas em algoritmos que garantem segurança na operação. A tecnologia de Blockchain tem se

inserido no mercado como uma solução viável em diversas áreas, sua estrutura de blocos apresenta uma operação assegurada por assinaturas digitais criptografadas, significando que os que emitem e recebem a transação estão protegidos, assim como os registros, conferindo transparência, imutabilidade e rastreamento em todas as etapas do processo.

Trata-se de um banco de dados distribuído numa rede distribuída ponto-a-ponto por um livro razão (*ledgers*), no qual não há unidade centralizadora e nenhum componente da rede possui prioridade quando comparado a outro. Sua unidade de software é composta de algoritmo que negocia o conteúdo informativo de blocos de dados ordenados e conectados, junto com tecnologias de criptografia e de segurança, a fim de prover e manter a sua integridade. Composta de três componentes: bloco de dados, razão distribuída e algoritmo de consenso.

7 VISÃO GERAL DA BLOCKCHAIN

Com a grande divulgação da tecnologia por Nakamoto (2008) no registro das transações do Bitcoin, inserido robustos mecanismo de segurança através de algoritmos que determinam regras de consensos, elevou-se o interesse pela pesquisa e aplicabilidade aos sistemas distribuídos estando hoje a Blockchain muito mais aperfeiçoada a partir de novas e constantes pesquisas e implementações. Mas para se ter uma visão da Blockchain, apresentamos um referencial teórico para que possamos entender o objetivo da pesquisa proposta.

Lin e Liao (2017) citam conceitos sobre Blockchain que as tecnologias Blockchain possuem técnicas de criptografia usando o algoritmo de consenso distribuído para resolver o problema tradicional de sincronização de banco de dados distribuído, com uma infraestrutura de nós integrados garantindo pelos recursos de:

Descentralização: Independente de um nó centralizado, os dados podem ser registrados, armazenados e atualizados distribuídos;

Transparência: O registro dos dados pelo sistema Blockchain é transparente para cada nó, também transparente na atualização dos dados, garantindo a confiabilidade;

Código aberto: A maioria dos sistemas de Blockchain é aberta a todos, o registro pode ser verificado publicamente e as pessoas também podem usar as tecnologias de Blockchain para criar qualquer aplicativo que desejarem;

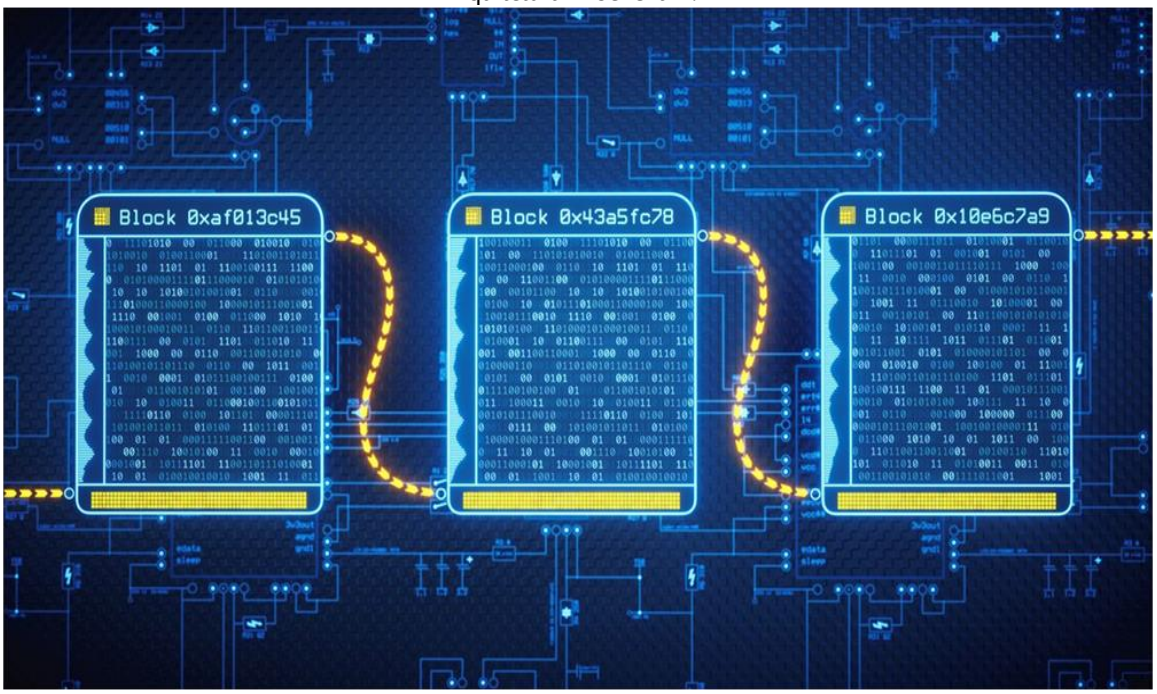
Autonomia: Por causa da base de consenso, todos os nós no sistema Blockchain podem transferir ou atualizar dados com segurança, a idéia é confiar em uma única pessoa para todo o sistema, e ninguém pode intervir; e

Imutabilidade: Característica marcante, ninguém pode modificar o livro-razão distribuído. Permanece irreversível, visto que qualquer transação não pode ser alterada, excluída ou revertida, a menos que mais de 51% dos nós concordem com a modificação.

8 ARQUITETURA BLOCKCHAIN

A arquitetura de um sistema de software determina como seus componentes estão organizados e como se relacionam. A visão entre um sistema centralizado e distribuído é declarada como sentidos opostos. Um sistema distribuído é composto de uma série de computadores interdependentes que cooperam uns com os outros usando um meio de comunicação a fim de atingir um objetivo específico, sem que haja um elemento centralizado para controle ou coordenação.

Arquitetura Blockchain.



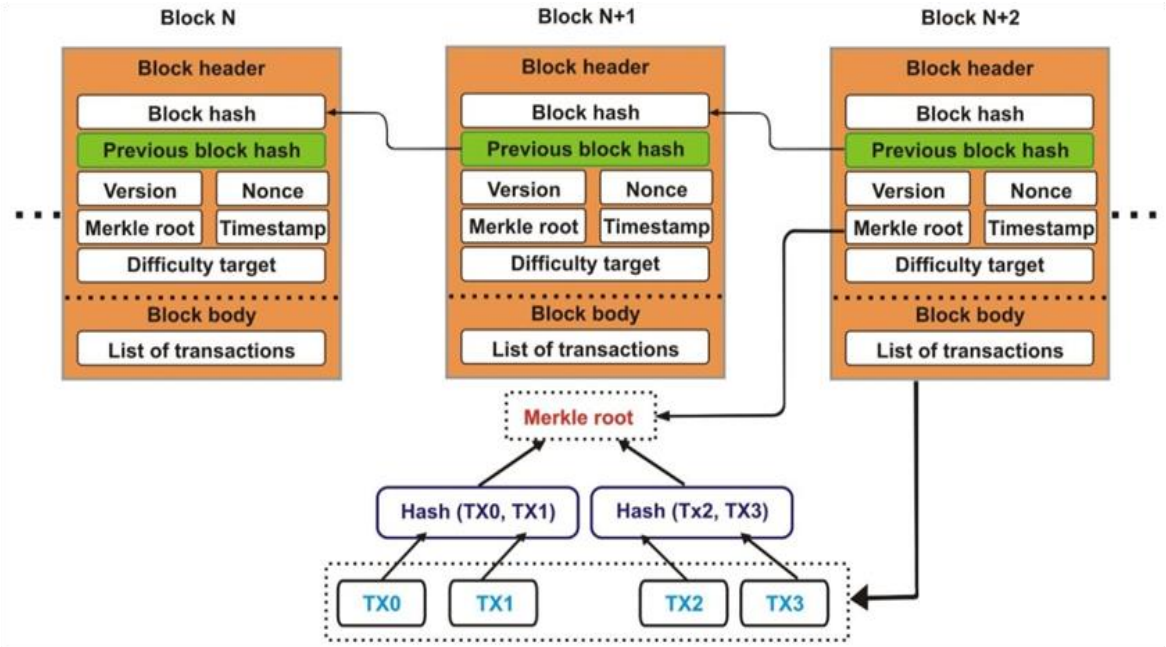
Fonte: Elaborada pelos Autores

Salman et al (2019) cita em seu trabalho a respeito da arquitetura da Blockchain: "*Consiste em um banco de dados e uma rede de nós, com dados compartilhados, distribuídos, tolerante a falhas e somente anexado que mantém os registros em blocos*".

Embora os blocos sejam acessíveis a todos os usuários da Blockchain, eles não podem ser excluídos ou alterados por eles. Os blocos são conectados entre si em uma cadeia, pois cada bloco possui valor de *hash* do seu predecessor. Cada bloco contém várias transações verificadas. Cada bloco inclui um registro de data e hora indicando a hora de criação desse bloco e um número aleatório (*nonce*) para operações criptográficas. Do ponto de vista da segurança, a cadeia de blocos é criada e mantida usando uma rede de sobreposição ponto a ponto e protegida por meio da utilização inteligente e descentralizada de criptografia.

9 ESTRUTURA DE BLOCOS

Estrutura de Blocos.



Fonte: Iqbal e Matulevičius (2021).

Ferreira, et alii.(2018), cita que os blocos são partes divididas em cabeçalho e as transações. O cabeçalho é composto de campos que armazenam dados como: hash do bloco anterior, dificuldade, *nonce* e raiz da árvore de Merkle. Os metadados possuem estrutura de altura do bloco e hash do cabeçalho, que identificam o bloco e sua posição na cadeia. As transações são o agrupamento dos dados que são armazenados no bloco. Uma vez armazenados os dados, eles são imutáveis, conferidos por um algoritmo que gera um código hash. Havendo alteração em ao menos um bit, o hash resultante será completamente diferente.

Sua estrutura dificulta a execução de ataques de modificação de blocos, visto que qualquer alteração na cadeia implica na mudança em todas outras cópias da Blockchain armazenadas por outros usuários. Para que um atacante possa controlar a criação de novos blocos, ele deve possuir mais de 50% do poder computacional de toda a rede. Somente assim seria possível criar blocos válidos com uma velocidade maior do que o resto dos usuários.

10 COMO FUNCIONA A BLOCKCHAIN

A Blockchain elimina intermediários confiáveis em um processo transacional e registra as transações em um livro-razão distribuído descentralizado em uma cadeia de blocos conforme Figura de Modelo de bloco, onde cada bloco se conecta a um bloco anterior por um *hash* criptográfico exclusivo. O primeiro bloco em um Blockchain é um bloco gênesis, cada bloco tem um cabeçalho e um corpo. O cabeçalho do bloco inclui um *hash* de bloco exclusivo, um *hash* de bloco anterior, raiz Merkle, versão do bloco, nonce, carimbo de data / hora e alvo de dificuldade. O corpo do bloco contém uma lista válida de transações que são *hash* ordenadas como uma árvore Merkle.

Cada dispositivo (computador, smartphone, etc) conectado à rede de uma Blockchain é chamado de nó, que contém uma cópia completa do banco de dados da aplicação para que possa validar e transmitir as transações aos demais nós. Os dados existentes no banco de dados não podem ser apagados ou alterados, visto que qualquer alteração nos dados será notificada para que aconteça uma nova validação dos blocos de dados, ou seja, um bloco que compõe a cadeia de blocos (Blockchain) está diretamente relacionado ao anterior e ao próximo, bem como o acesso a todos os blocos do banco de dados, gerando confiabilidade e facilidade para uma eventual auditoria.

Tipos de Redes Blockchain.

Tipos de Redes Blockchain				
	Pública	***Privada***	***Consórcio***	***Híbrida***
Vantagens	***. Transparência . Independência . Confiança***	***. Controle de Acesso . Performance***	***. Controle de Acesso . Performance . Escalabilidade***	***. Controle de Acesso . Segurança . Escalabilidade***
Desvantagens	***. Performance . Escalabilidade . Segurança***	***. Confiança . Auditabilidade***	***. Transparência . Atualização***	***. Transparência***

Aplicação	***. Criptomoedas . Validação de documentos***	***. Propriedade de Ativos . Cadeia de Suprimentos***	***. Registros médicos . Registro de imóveis***	***. Registro financeiro, bancário e cadeia de suprimentos.***

Fonte:elaborado pelos autores.

Iqbal e Matulevičius (2021) citam que as redes Blockchain são categorizadas com ou sem permissão. Exemplo de redes abertas sem permissão, Bitcoin e Ethereum. Com permissão temos exemplo, Hyper Ledger Fabric (HLF), Corda. Por sua vez, Wust e Gervais (Jun. 2018), citam que em redes Blockchain sem permissão, qualquer pessoa no mundo pode ingressar na rede, não há necessidade de permissões para participar do consenso ou executar uma transação. As transações nessas redes são visíveis publicamente para todos. Redes Blockchains permitidas, apenas nós pré-verificados podem entrar na rede, a camada de controle de acesso controla as operações dos participantes da rede e a visibilidade da transação é restrita. São quatro tipos principais de redes de Blockchain, com suas vantagens, desvantagens e usos para uma determinada aplicação: Blockchains Públicas, Privadas, Consórcio e Híbrida.

11 MINERAÇÃO DE BLOCOS

Spengler e Souza (2021) cita que o processo de criação de um bloco é denominado mineração, sendo o mecanismo pelo qual os registros são validados. Esse nome deve-se ao fato do processo se assemelhar ao modo como outros produtos de valor, como ouro, são extraídos, devido ao esforço dedicado nesse trabalho. Ao ser propagado pela rede, o novo bloco é inserido na cópia local da cadeia de todos os nós participantes da rede Antonopoulos (2017) Antes de inserir o bloco na cópia local, o nó realiza a verificação de cada transação armazenada pelo bloco. Cada um desses ‘nós’ pode armazenar uma cópia exata de todos os dados das transações realizadas, então, quando um novo ‘nó’ é adicionado, ele pode receber uma cópia dos dados armazenados em outros nós, garantindo que quando o inverso acontece, não haja impactos na rede. Após a execução dessa etapa, se todas as transações foram consideradas válidas, o nó adiciona o bloco na sua cópia local da Blockchain. Dessa forma, o processo de validação ocorre em duas etapas, a primeira na validação das transações e a segunda na validação do bloco. Após os dados serem inseridos na cadeia eles tornam-se imutáveis.

12 GASTO DUPLO

Refere-se a uma falha nas primeiras variantes do sistema de dinheiro digital, em que uma única moeda digital pode ser gasta mais de uma vez. No entanto, em um mecanismo descentralizado sem o banco ou um intermediário central, é difícil acompanhar a propriedade. Mecanismos de consenso resolvem o problema do gasto duplo ao rastrear a propriedade das moedas do bloco de gênese, o primeiro bloco na Blockchain. Se você gastar uma moeda, a propriedade muda e a transação é registrada.

13 CRIPTOGRAFIA DE CHAVES ASSIMÉTRICAS E A FUNÇÃO HASH

A criptografia de chaves e a função *hash* são os principais elementos da criptografia, por ser uma função matemática de mão única, mas de dificuldade extrema para fazer o caminho oposto. Existem muitas funções de *hash* diferentes entre si no que concerne ao tamanho do valor de *hash* que geram. Os valores de *hash* podem ser usados para comparar dados, detectar se os dados que se supõe permanecem inalterados, referenciar dados de modo sensível a mudanças, armazenar um conjunto de dados de modo sensível a mudanças e criar tarefas custosas do ponto de vista do processamento. A criptografia tem o objetivo principal de proteger os dados contra acessos por pessoas não autorizadas visando proteger os dados transformando-os em um texto cifrado, usando uma chave de criptografia. Descriptografar é transformar o texto cifrado de volta em dados úteis, utilizando uma chave de criptografia correspondente.

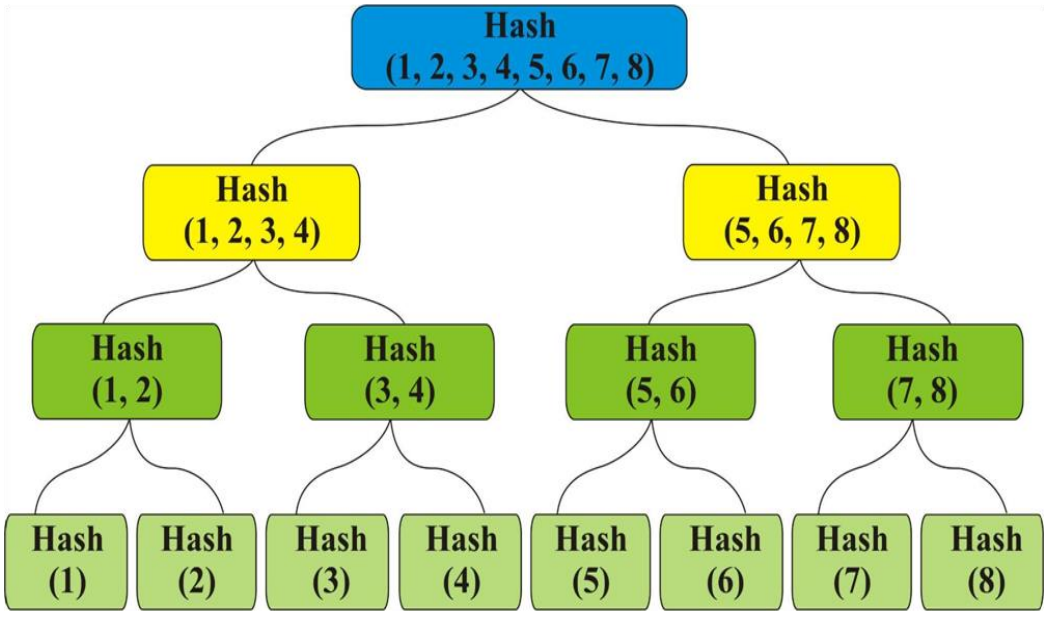
Salman et al. (2019) definem que a criptografia assimétrica ou criptografia de chave pública é uma técnica criptográfica que usa um par de chaves, as chaves públicas que são distribuídas pelo sistema e chaves privadas que são mantidas em segredo. A criptografia assimétrica sempre utiliza duas chaves complementares: o texto cifrado criado com uma dessas chaves só poderá ser descriptografado com a outra chave, e vice-versa. Quando a criptografia assimétrica é usada na vida real, essas chaves, em geral, são chamadas de chave pública e chave privada para enfatizar suas funções. A chave pública é compartilhada com todos, enquanto a chave privada é mantida em segredo. Por esse motivo, a criptografia assimétrica também é conhecida como criptografia de chave pública e privada. A chave pública é usada por todos criptografar dados, que só poderão ser descriptografados pelo proprietário da chave privada correspondente. É o equivalente digital de uma caixa de correio pública, na qual todos podem colocar cartas, mas somente o proprietário pode abri-la. A Blockchain utiliza a criptografia assimétrica para alcançar dois objetivos: Identificar contas de usuário e autorizar transações uma vez que o

proprietário da conta que transfere a posse cria um texto cifrado com a chave privada correspondente.

14 ÁRVORE DE MERKLE

A Teoría de Merkle (Merkle, 1982), aplicado à Blockchain, consiste em uma estrutura de dados que utiliza uma representação resumida sobre todos os valores *hash* de transações armazenadas em um bloco para garantir a integridade de um conjunto de dados de uma árvore binária, através da concatenação de valores *hash* de blocos vizinhos, recursivamente até que se chegue ao *hash* do bloco raiz. Definida como uma árvore de pesquisa binária com seus nós de árvore vinculadas umas a outras usando ponteiros de *hash*, agrupando esses nós em grupos separados, de modo que cada vez que dois nós no nível inferior são agrupados em um no nível pai, e para cada par de nós de nível inferior, o algoritmo de construção de árvore Merkle está criando um novo nó de dados, que contém o valor *hash* de cada um. Este processo se repete até chegar à raiz da árvore. O valor do *hash* raiz é então armazenado na área de cabeçalho de um bloco e cada participante da rede, visando reconstruir a árvore para a verificação e, consequentemente, a validação das transações contidas no bloco, conforme cita Nakamoto (2008). Havendo alteração em alguma transação da árvore, o novo *hash* gerado invalida toda a cadeia de blocos e em consequência a operação é invalidada, conforme a Propriedade de Imutabilidade dos Blocos.

Árvore de Merkle.



Fonte: Ferreira, et alii. (2017).

A árvore de Merkle tem a capacidade de impedir que os dados sejam adulterados, percorrendo os ponteiros de hash para qualquer nó na árvore. Especificamente, quando um adversário tenta adulterar dados em um nó folha, isso causará uma mudança no valor de hash se ele continuar a adulterar o nó superior, ele precisa alterar todos os nós no caminho de baixo para cima. Pode-se detectar facilmente que os dados foram adulterados, uma vez que o ponteiro de *hash* do nó raiz não corresponde ao ponteiro de *hash* que foi armazenado.

Uma vantagem é que ela pode provar de forma eficaz e concisa a associação de um nó de dados, mostrando esse nó de dados e todos os seus nós ancestrais em seu caminho ascendente até o nó raiz. A associação da árvore Merkle pode ser verificada em tempo logarítmico computando hashes no caminho e verificando o valor do *hash* em relação à raiz.

15 TECNOLOGIA DE REGISTROS DISTRIBUÍDOS (DLT-DISTRIBUTED LEDGER TECHNOLOGY)

Embora Blockchain e DLT (sigla para “Distributed Ledger Technology” ou tecnologia de registros distribuídos) confundem-se como sinônimos, mas na verdade são elementos diferentes. Ledger é o termo em inglês para “livro-razão” ou “registro contábil” que compõe os blocos da Blockchain que se referem a um registro de informações distribuídos por uma rede, garantindo maior grau de transparência de informações ante ao sistema tradicional centralizado. Em resumo, DLT são tecnologias de ledger distribuído é um banco de dados digital com informações copiadas, compartilhadas e sincronizadas, espalhadas geograficamente por vários pontos, ou seja, os os nós em um ecossistema ou rede, que operam sem um administrador central como em um banco de dados padrão que utilizam algoritmos de consensos como POW, POS, entre outros. Esses algoritmos de consensos determinam como novos blocos são adicionados. O processo de autenticação na rede para a escrita no ledger, ou seu livro razão de blocos, se dá através de outro método criptográfico que é a Assinatura Digital. A posse de uma chave privada permite gerenciar o acesso a endereços e auxiliar na realização de transações em DLT.

16 MECANISMOS DE CONSENSOS

Lashkari e Musilek (2021), pela origem dos livros-razão, foram encontrados documentos existentes a milhares de anos de operações correlatas. Sua formalização deu-se a partir da criação do sistema bancário convencional em que os registros de dados

foram autenticados por uma autoridade central. Com o surgimento do processamento eletrônico de dados em computadores, os livros-razão foram digitalizados, evoluindo ao que conhecemos como sistema de contabilidade centralizado. Nakamoto (2008) lança a idéia de exclusão de ambientes sem autoridade central a partir das tecnologias de SD em uma estrutura verificável a partir das DLT, que possibilitaram uma nova forma de registrar transações usando criptografia, algoritmos avançados e enorme capacidade de computação de forma segura e auditável, sem haver a necessidade de uma entidade que homologue a transação, aplicado às Blockchains, suas transações são legitimadas através dos mecanismos de consenso.

Mecanismos de Consensos são protocolos que garantem que todos os nós estão sincronizados entre si e concordam sobre quais transações são legítimas e são adicionadas na Blockchain. Esses mecanismos de consenso são cruciais para que uma Blockchain funcione corretamente. Eles garantem que todos usem a mesma Blockchain. Todos podem enviar coisas para serem adicionadas à Blockchain, então é necessário que todas as transações sejam verificadas constantemente e que a Blockchain seja constantemente auditada por todos os nós. Sem um bom mecanismo de consenso, os Blockchains correm o risco de vários ataques.

17 CONTRATOS INTELIGENTES

Observa-se um aumento exponencial de aplicações em Blockchain na última década, conforme cita Lone e Naaz (2021). Um dos principais motivos deve-se a sua própria arquitetura, baseada em características como a descentralização, possibilidade de anonimato e confiança na aplicação. Com a implementação de regras e funcionalidades capazes de executar sozinha negociação entre duas ou mais partes, prescindindo de intermediários centralizados, esses códigos podem definir tarefas, estabelecendo as obrigações, benefícios e penalidades que podem ser devidas a qualquer das partes em várias circunstâncias diferentes, proporcionando confiabilidade nas relações entre a rede, da mesma forma que um documento legal tradicional. A essas regras deu-se a denominação de Contratos Inteligentes que diferente de um contrato tradicional escrito em linguagem puramente jurídico-legal, um contrato inteligente é capaz de obter informações, processá-las e tomar as devidas ações previstas de acordo com as regras do contrato.

O Ethereum, como uma das principais tecnologias de Blockchain baseada em contratos inteligentes, impulsionou de forma significativa a utilização de contratos

inteligentes nas aplicações além das criptomoedas, entretanto, pela rapidez como as novas aplicações estão surgindo, desafios e futuras direções de pesquisa no campo da aplicação de contratos inteligentes em especial na proteção de Internet e IoT estão se destacando. O Ethereum é uma plataforma de Blockchain de código aberto que combina o Smart Contract, oferecendo máquina virtual descentralizada para lidar com o contrato, usando sua moeda digital chamada ETH, as pessoas podem criar muitos serviços, aplicativos ou contratos diferentes nessa plataforma.

18 DESAFIOS DA TECNOLOGIA DE BLOCKCHAIN

Embora a Blockchain tenha grande potencial, alguns desafios devem ser considerados em sua adoção quanto à tecnologia para atender a uma demanda. Elencamos alguns aspectos a serem analisados quando da adoção da tecnologia. Embora tenhamos observado um elevado número de aplicativos Blockchain, sua implementação não é tão simples, bem como o que observamos a respeito de seu desempenho. A segurança é um ponto forte, embora nesta tese discutíssemos alguns elementos de preocupação que formam o objetivo de nosso trabalho.

A Tabela abaixo de *Análise comparativa entre plataformas Centralizadas e Blockchain*, apresenta uma análise comparativa entre sistemas centralizados e aplicações Blockchain em diversos aspectos.

Análise comparativa entre sistemas centralizados e aplicações Blockchain.

ÁLISE COMPARATIVA ENTRE PLATAFORMAS CENTRALIZADAS E BLOCKCHAIN		
ASPECTOS	**PLATAFORMA CENTRALIZADA TRADICIONAL**	**PLATAFORMA DISTRIBUÍDA Blockchain**
Manipulação de dados	Suporte para as quatro operações: **Criar, Ler, Atualizar e Excluir**.	Disponível nas operações de **Leitura e Gravação.**
Autoridade	**Centralizada**: controlada por uma entidade administradora.	**Descentralizada**.
Integridade	Permitem **alteração e exclusão**.	**Dados imutáveis.**
Privacidade	**Maior vulnerabilidade de ataques** mal-intencionados.	Dados criptografados que possibilitam **mais proteção**.
Transparência	**Possibilidade de dados não transparentes.**	Por estarem em uma rede distribuída, **permitem maior transparência.**
Garantia de Qualidade	Necessidade de **autenticação por uma entidade administradora.**	Dados rastreáveis desde sua origem **garantem imutabilidade protegidos** por criptografias com Hash de dados.

Tolerância a falhas	**Alto risco** de pena em ponto único.	**Tolerância a falhas** em sua arquitetura de projeto.
Custos	**Fácil de implementar e manter.**	Por não ser de grande domínio, **maior custo de desenvolvimento e manutenção.**
Desempenho	**Maior rapidez em transações** processadas e maior escalabilidade.	**Menor desempenho** pela menor quantidade de aplicações desenvolvidas, possibilidade de melhoria ao longo de novos projetos.
Força de trabalho	**Elevado número de Profissionais** em diversas plataformas de sistemas tradicionais centralizados.	**Escassez de mão de obra qualificada** para desenvolvimento e suporte a aplicações Blockchain.
Escalabilidade	**De fácil atualização**, permite adoção da escalabilidade sem grandes modificações, como tamanho dos registros e aumento no número de transações.	**Um desafio à Blockchain** visto que por sua natureza de registros fixos imutáveis e maior tempo de processamento nas transações.
Legislação	Regulamentado pelo RGPD.	Controvérsias quanto à aplicação do **RGPD**.

Fonte: Elaborado pelos autores.

19 ECOSSISTEMAS BLOCKCHAIN, APLICATIVOS E ESTUDOS DE CASOS

A utilização de DApps baseados em Blockchains fazem-se presentes em diferentes áreas, como os serviços de monitoramento e segurança de rede, que utilizam as funções de autenticação, confidencialidade, privacidade, integridade e procedência sem a necessidade de corretores terceirizados confiáveis, que é um dos principais incentivos ao desenvolvimento de soluções autônomas e independentes baseados na abordagem dos contratos inteligentes que definem previamente as regras do negócio de maneira transparente e segura.

Revoredo (2019) comenta a respeito da aplicabilidade da Blockchain em soluções que necessitam maior ênfase na confiança de seus dados, ou seja, aplicação que tenha proteção e garanta uma transação segura sem intermediários pela sua natureza de desconfiança mútua pelas partes envolvidas. Os Ativos armazenados nos sistemas podem ser tangíveis (por exemplo, dinheiro, casas, carros, terras) ou intangíveis (por exemplo, direitos autorais, documentos digitais e direitos de propriedade intelectual). Entre exemplos desses modelos de aplicações temos: Prontuário Médico, Estabelecimento de Contratos, Estabelecimento de Identidade Digital, Cartórios Digitais, Registro de Propriedade Intelectual, Operações Cambiais Imediatas e Sistema de Voto Digital.

Adiciona-se a listas de aplicações que atendem bem ao requisito citado como: Pagamentos, Criptomoedas, Rastreabilidade na cadeia de suprimentos, Rastreabilidade na produção de alimentos, Bens digitais, Conformidade e auditoria, Impostos, Combate a notícias falsas,

entre outras aplicações.

20 CRIPTOMOEDAS

Definido como um bem digital, desenhado para funcionar como meio de troca onde em um banco de dados distribuído em que as informações estão criptografadas e espalhadas por toda a rede. A idéia de uma moeda digital foi definida por Shamir (1984), David Chaum, que lançou o conceito de moeda digital anônima e criptografada e a denominou de "ecash", implementado em 1995 o Digicash, uma forma inicial de criptomoeda que podia ser controlada e enviada a outras pessoas, mas tudo por um sistema digital e que garantia o anonimato ao proprietário. Em 1996, a NSA (*National Security Agency*), agência de segurança nacional dos Estados Unidos, publicou um artigo descrevendo esse sistema e expondo a preocupação com o fato de permitir o anonimato e as implicações disso para o combate ao crime. Dois anos mais tarde, Wei Dai, um engenheiro de computação, conhecido por sua contribuição ao sistema de criptos, criou a Crypto++, uma série de protocolos e programas, além de implementar o b-money e o VMAC, sistemas que ajudam as criptomoedas a existirem.

Nakamoto (2008), lança o movimento sobre as criptomoedas atribuindo ao codinome de Satoshi Nakamoto no qual descreve um sistema descentralizado, sem controle por um organismo central como banco central ou governo, que não dependesse de instituições físicas, nem se submetesse a regulamentações de um governo específico e sim a regras denominadas de Regras de Consensos. Somente em 2009 é que aparece o Bitcoin, protegido por criptografía SHA-256. A obra de Nakamoto (2008) foi a base para o protocolo de consenso que conhecemos hoje, que é o PoW. Como expomos, tal qual a Blockchain, as criptomoedas não houve um único inventor e sim uma evolução de diversas tecnologias. Cada uma dessas tecnologias coloca em destaque alguns autores como o Bitcoin atribuído a Satoshi Nakamoto e Ethereum à Vitalik Buterin.

Mattos; Abouchedid e Silva (2020) afirmam que apesar do aumento da aceitação e do volume de transações denominadas nessa criptomoeda, as valorizações abruptas e intensas e as grandes variações diárias na cotação em relação ao dólar sugerem um comportamento semelhante ao de um ativo utilizado, principalmente, para fins especulativos. Na sua concepção original, o Bitcoin conseguiria fazer frente à moeda emitida pelos Estados, servindo como unidade de conta, meio de troca e reserva de valor. No entanto, uma análise mais cuidadosa das características de instrumentos monetários em uma economia capitalista contemporânea sugere que dificilmente a moeda estatal será

substituída por criptomoedas, embora haja um potencial significativo para o uso dessas tecnologias em um sistema de pagamento coordenado pelos Bancos Centrais.

21 BITCOIN

Sistema de pagamento ponto a ponto descentralizado que usa criptomoeda denominada Bitcoins (BTC) e foi lançado como software de código aberto em 2009. Ao contrário das moedas fiduciárias, não há autoridade centralizada ou qualquer reconhecimento estatutário, apoio ou regulamentação. Todas as transações são confirmadas e validadas por um esquema de consenso, possibilitado por um organizado sistema coletivo de nós conhecido como "mineração". Os mineradores confirmam cada transação para autenticidade. Isso aumenta a segurança no sistema Bitcoin e garante a filosofia central do Bitcoin "*Manter a confiança em um ambiente não confiável*", sem a necessidade de um terceiro de confiança como recompensa, os mineradores coletam taxas de transação para as transações que eles confirmam. A plataforma Bitcoin atraiu elementos sociais e anti-sociais. Por um lado, é social, pois garante a troca de valor, mantendo a confiança de forma cooperativa e voltada para a comunidade, sem a necessidade de um terceiro de confiança. Ao mesmo tempo, é antissocial, pois cria obstáculos para a aplicação da lei rastrear transações suspeitas devido ao anonimato e à privacidade conforme cita Nerurkar et al. (2021).

Documento publicado em Bitcoin-Open source P2P Money (2009) descreve Bitcoin como uma P2P usando o mecanismo de Consenso PoW para gravar um histórico público de transações que rapidamente se torna computacionalmente impraticável para um atacante para mudar se nós honestos controlarem a maioria do poder de CPU. A respeito dos nós: trabalham todos de uma vez, com pouca coordenação. Quanto à privacidade, os participantes da rede não precisam ser identificados, uma vez que as mensagens não são roteadas para qualquer lugar particular e só precisam ser apresentadas em regime de melhor esforço. Os nós podem sair e voltar à rede à vontade, aceitando a cadeia de prova de trabalho, como prova do que aconteceu enquanto eles estavam fora. Eles votam com seu poder de CPU, expressando a aceitação de blocos válidos, trabalhando em estendê-los e rejeitando blocos inválidos, recusando-se a trabalhar com eles. Todas as regras e incentivos necessários podem ser aplicados com este mecanismo de consenso.

22 ETHEREUM

Plataforma de software baseada em Blockchain que possibilita a construção e execução de contratos inteligentes para os DApps. Essa plataforma também é a base da moeda virtual Ether. Com esta criptomoeda é possível fazer pagamentos a outras contas ou às máquinas que executem alguma operação solicitada. Ethereum fornece uma linguagem de programação Turing completa que permite definir os contratos inteligentes, criar programas e executá-los na Blockchain.

Opera usando contas e saldos, que mudam por meio de transições de estado. O estado denota os saldos atuais de todas as contas, além de outros dados extras possíveis. O estado não é armazenado na Blockchain diretamente, mas é codificado e mantido por contas em uma estrutura de dados separada organizada como uma árvore Merkle. Como em todos os Blockchains sem permissão, para fornecer anonimato, as contas são pseudônimos e estão vinculadas a um ou mais endereços.

Existem dois tipos de contas, as de propriedade externa e de contratos. As contas externas são controladas por pessoas. Assim, semelhante ao Bitcoin, cada pessoa tem sua própria chave privada, que é usada para fazer transações na Blockchain Ethereum. Por outro lado, as contas de contrato são controladas por algum código de contrato inteligente. Ou seja, tais contas são uma espécie de cyber entidades, com saldo próprio, que podem ser acionadas através de algumas transações, oriundas de uma conta externa (ou de alguns outros contratos). Uma vez acionado, o código especificado no contrato é executado. Este código pode, por sua vez, gerar algumas outras transações. Os contratos inteligentes permitem que os desenvolvedores usem Ethereum como uma estrutura de propósito geral para criar DApps conforme cita Ferretti e D'Angelo (2020).

23 COMPARATIVO ENTRE ETHEREUM E BITCOIN

Revista Plus500 (2022) cita que Ether, a moeda usada para efetuar transações na rede Ethereum (saber mais) e a Bitcoin têm muitas semelhanças fundamentais. São ambas criptomoedas que estão enraizadas na tecnologia Blockchain. Isso significa que computadores independentes por todo o mundo se voluntariam para manter uma lista de transações, permitindo que o histórico de cada moeda seja verificado e confirmado. Ambas são moedas virtuais usadas ativamente para serviços, contratos e como reserva de valor. A sua popularidade chamou a atenção de publicações de notícias e investidores que esperam entender melhor como a tecnologia de Blockchain pode mudar o cenário monetário com o tempo. É aqui que termina a maioria das semelhanças. A sua natureza

descentralizada é uma grande mudança em relação às moedas tradicionais, mas elas não são aceites em todos os locais. Embora a Bitcoin seja mais amplamente aceita e vista como uma moeda digital internacional, a Ether só é aceite para transações de Aplicativos Digitais (Dapps) que circulam na rede Ethereum.

24 A ERA PRÉ-BLOCKCHAIN

Sherman et al. (2019) citam que embora o artigo seminal sobre Bitcoin tenha aparecido em 2008 com o misterioso autor Satoshi Nakamoto, Nakamoto (2008), a maioria das ideias tecnológicas subjacentes surgiram muitos anos antes. Autores como Chaum (1982), Merkle (1979), Merkle (1982) e Stuart e Stornetta (1990) deram grandes contribuições na evolução da Blockchain. A ideia de uma construção subjacente à prova de trabalho (PoW) permitiu ao Bitcoin utilizar a primeira PoW para mineração e obtenção de consenso. Merkle (1978) propôs para implementar a criptografia de chave pública.

Leslie Lamport, tem um destaque especial na construção do que temos hoje na Blockchain, diversos trabalhos apresentados tornaram-se referência entre eles estão em Lamport (1978) que apresentou o conceito de replicação de máquina de estado (Byzantine fail-tolerant (BFT)) aplicado à Blockchains autorizadas, posteriormente formalizada de forma concisa por Schneider (1990). A replicação da máquina de estado especifica quais são as transações e em que ordem elas são processadas, mesmo na presença de falhas (bizantinas) e comunicações não confiáveis foram observadas por Lamport; Shostak e Pease (1982). Para alcançar uma forte forma de consenso de transação, muitos sistemas permissionados baseiam-se nas ideias do protocolo Paxos de 1998 de Lamport (1998) que lida apenas com falhas de travamento e do protocolo PBFT apresentado por Castro e Liskov (2002). Importante contribuição em Nakamoto (2008a) para o sistema Bitcoin sem permissão na realização do acordo bizantino em redes abertas.

25 CRONOLOGIA PARA A FORMAÇÃO DA BLOCKCHAIN

Uma breve história da blockchain

Ano	Contribuição científica para o desenvolvimento da Blockchain
1970	• ***James Ellis***, criptografia de chave pública descoberta no GCHQ em segredo;
1973	• ***Clifford Cocks***, criptosistema RSA descoberto no GCHQ em segredo;
1974	• ***Ralph Merkle***, enigmas criptográficos (artigo publicado em 1978);

1976	• ***Diffie e Hellman***, criptografia de chave pública descoberta em Stanford;
1977	• ***Rivest, Shamir e Adleman***, sistema criptográfico RSA inventado no MIT;
1979	• ***David Chaum***, cofres e compartilhamento secreto (dissertação 1982);
1982	• ***Lamport, Shostak e Pease***, Problema dos Generais Bizantinos;
1991	• ***Stuart Haber e W Scott Stornetta,*** Uma cadeia de blocos criptograficamente protegida é descrita pela primeira;
1992	• ***Dwork e Naor***, combatendo lixo eletrônico;
1994	• ***Szabo,*** Cunhou o termo "contrato inteligente";
1998	• ***Nick Szabo,*** Apresentou o trabalha 'bit gold', uma moeda digital descentralizada;
2000	• ***Stefan Konst,*** Publica sua teoria de cadeias seguras criptográficas, além de ideias para implementação;
2002	• ***Adam Bach,*** Apresenta o Hashcash;
2008	• ***Nakamoto, S.(2008),*** O(s) desenvolvedor(es) trabalhando sob o pseudônimo de Satoshi Nakamoto lançam um white paper estabelecendo o modelo para um blockchain;
2009	• ***Nakamoto,*** Implementa a primeira blockchain como livro-razão público para transações feitas com Bitcoin;
2014	• ***A tecnologia Blockchain,*** É separada da moeda e seu potencial para outras transações financeiras interorganizacionais é explorado. Nasce o Blockchain 2.0, referindo-se a aplicações além da moeda; • ***O sistema Blockchain Ethereum,*** Introduz programas de computador nos blocos, representando instrumentos financeiros como títulos conhecidos como contratos inteligentes;
2017	• ***Wright e Savanah***, pedido de patente europeia nChain (emitido em 2018);
2018	• ***Blockchains híbridos***, que combinam replicação de máquina de estado tolerante a falhas bizantinas com defesas contra ataques Sybil; • ***Hyperledger,*** Projeto guarda-chuva envolvendo Fabric, um sistema para blockchains autorizados; • ***Ethereum,*** Plataforma para blockchains públicos;

Fonte: Sherman; Javani; Zhang and Golaszewski (2019).

26 O FUTURO DA BLOCKCHAIN

Modelo simulado para Cidades Inteligentes.

Fonte: Elaborado pelos autores.

A rápida aceitação da inteligência artificial (IA) como elemento de transformação social, tecnológica e científica poderá integrar a Blockchain na criação de ecossistemas digitais, com ajuda de dispositivos de IoT para que possamos ter um número maior de Cidades Inteligentes, em áreas que variam de serviços financeiros, sociais e públicos, baseados na segurança dos dados e informações podem garantir maiores inovações em tecnologias a partir das respostas aos desafios que estão por vir.

Novas oportunidades de força de trabalho na forma de empregos e rendas serão as oportunidades que podem ser alcançadas no processo de desenvolvimento de cidades inteligentes, que irão fomentar inovações em tecnologias, tendo a Blockchain como ferramenta de apoio ao combate aos problemas de segurança e garantia de preservação de dados, com um importante papel nos desafios que encontraremos à frente.

27 CONCLUSÃO

A Blockchain tem se destacado em diferentes aplicações como uma proposta para novos modelos de negócios, em contraponto aos sistemas centralizados. Há que se considerar estudos para que se evoluam cada vez mais questionamentos como: desempenho em elevado volume de dados, segurança, confiabilidade e privacidade dos dados, em especial quando aplicados aos ecossistemas de IoT e a integração com a IA (Inteligência Artificial).

Apresentamos neste artigo, um relato a respeito da origem da tecnologia e seu futuro, de forma a garantir como uma proposta a ser avaliada quando da elaboração de projetos de tecnologias nas organizações. Sua utilização em casos específicos de utilização é um fator a ser levado em conta, por não se tratar de um *framework* genérico gerador de sistemas informáticos capaz de resolver qualquer problema que envolva as tecnologias da informação e comunicação. Esse artigo teve o caráter explicativo a respeito de se conhecer com mais profundidade a tecnologia que não é uma inovação nem uma novidade tecnológica e sim uma ferramenta capaz de integrar diferentes outras tecnologias como citado a partir de uma arquitetura sólida capaz de garantir a segurança dos dados armazenados a partir de fortes algoritmos matemáticos em formato de mecanismos de consensos, capazes de suportar a continuidade nos negócios contra as ameaças de segurança cada vez maiores, fator de grande importância no contexto tecnológico atual.

O artigo discorreu brevemente sua história, a forma de seu funcionamento e sua relação com o Bitcoin. No entanto, o foco principal do artigo é a tecnologia Blockchain e não nas criptomoedas virtuais e, por isso, explica também suas características e limitações, visando compreender quais são os benefícios da implementação desta tecnologia em aplicações de diversas áreas.

Concluiu-se que tal tecnologia apresenta inúmeras possibilidades de aplicações em áreas além das criptomoedas virtuais, garantindo maior segurança e menor custo a partir de várias iniciativas que possibilitam uma revolução da distribuição de dados atuais na qual a tecnologia Blockchain encontra-se como protagonista e em constante evolução.

REFERÊNCIAS

Antonopoulos, A. M.(2017). *Mastering Bitcoin: Programming the Open Blockchain.* O'Reilly Media, Inc., 2nd edition.

Bitcoin - Open source P2P money.(2009). [Na Internet]. Disponível em: <https://bitcoin.org/en>. [Consultado em 10/02/2023].

Blockchain Case.(2020). *Can Blockchain Technology Solve The Problem Of Illegal Fishing.*[Na Internet]. Disponível em: < https://www:investopedia:com/news/can-Blockchaintechnology-solve-problem-illegal-fishing>.[Consultado em 09/02/2023].

Castro, M., and B. Liskov, B.(2002). *Practical Byzantine fault tolerance and proactive recovery.* ACM Transactions on Computer Systems, Vol. 20, No. 4 (November 2002), 398-461.

Chaum, D. L.(1982). *Computer systems established, maintained and trusted by mutually suspicious groups.* Ph.D. dissertation, University of California, Berkeley (April 1982).

Coulouris, G., Dollimore, J. and Kindberg, T.(2007). *Sistemas distribuídos: conceitos e projeto.* 4. ed. Tradução de João Tortello. Porto Alegre: Bookman.

Ethereum Project.(2021). [Na Internet]. Disponível em: <https://www.ethereum.org/>. [Consultado em 23/10/2021].

Ethereum WritePaper.(2021). Ethereum WritePaper. [Na Internet]. Disponível em: <https://www.ethereum.org/en/writepaper>. [Consultado em 17/12/2022].

Ferreira, J., Pinto, F. & Santos, C.(2017). Estudo de mapeamento sistemático sobre as tendências e desafios do blockchain. Revista Eletrônica Geral Organizacional. Recife, v.15, Edição Especial, p. 108-117.

Ferreira, E., Albuquerque, C., Rocha, A. & Chicarino, V. R. L.(2018). *Uso de Blockchain para Privacidade e Segurança em Internet das Coisas.* [Na Internet]. Disponível em:<https://www.repositorio.mar.mil.br/handle/ripcmb/844281>. [Consultado em 10/08/2020].

Ferretti, S. & D'Angelo, G.(2020). *On the Ethereum Blockchain structure: A complex networks theory perspective.* [Na Internet]. Disponível em: <https://onlinelibrary.wiley.com/action/showCitFormats?doi=10.1002%2Fcpe.5493>. [Consultado em 16/11/2021].

Hyperledger Project.(2021). Hyperledgert Project. [Na Internet]. Disponível em: <https://www.hyperledger.org>. [Consultado em 02/11/2022].

Hyperledger, IBM Blockchain.(2020). *IBM Blockchain based on Hyperledger Fabric from the Linux Foundation.* [Na Internet]. Disponível em:<https://www.ibm.com/Blockchain/hyperledger.html>. [Consultado em 22/01/2023].

Iqbal, M. & Matulevičius, R.(2021). *Exploring Sybil and Double-Spending Risks in Blockchain Systems*, in IEEE Access, vol. 9, pp. 76153-76177, 2021, doi: 10.1109/ACCESS.2021.3081998.

Lamport, L.(1978). *Time, clocks and the ordering of events in a distributed system.* Communications of the ACM, Vol. 21, No. 7 (1978), 558–565.

Lamport, L., Shostak, R. and Pease, M.(1982). *The Byzantine Generals Problem.* Trans. on Programming Languages and Systems, Vol. 4, No. 3 (July 1982), 382-401.

Lamport, L.(1998). The part-time parliament. ACM Transactions on Computer Systems, Vol. 16, No. 2 (May 1998), 133-169.

Lashkari, B. & Musilek, P.(2021). *A Comprehensive Review of Blockchain Consensus Mechanisms in IEEE* Access. vol. 9, pp. 43620-43652. [Na Internet]. Disponível em: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9376868>. [Consultado em 15/04/2020].

Lima, C.(2018). *Developing Open and Interoperable DLT/Blockchain Standards.* Computer 2018, 51, 106–111.

Lin, I. C. and Liao, T. C.(2017). *A Survey of Blockchain Security Issues and Challenges.* IJ Network Security, 19(5), 653-659.

Lin L., Liao T. and Corresponding author: Iuon-Chang Lin.(2017). *A Survey of Blockchain Security Issues and Challenges.* [Na Internet]. Disponível em: <http://ijns.jalaxy.com.tw/contents/ijns-v19-n5/ijns-2017-v19-n5-p653-659.pdf> [Consultado em 17/12/2022].

Lone, A. H. Lone & Naaz, R.(2021). *Applicability of Blockchain smart contracts in securing Internet and IoT: A systematic literature review*, Computer Science Review, Volume 39, 100360,
ISSN 1574-0137. [Na Internet]. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1574013720304603> [Consultado em 19/10/2019].

Majeed, U., Khan, L.U., Yaqoob, I., Kazmi, S.M.A., Salah, K., Hong, C.S.(2021). Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges, Journal of Network and Computer Applications. Volume 181, 103007, ISSN 1084-8045,
https://doi.org/10.1016/j.jnca.2021.103007. [Na Internet]. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1084804521000345>. [Consultado em 02/07/2022].

Mattos, O. B., Abouchedid, S. & Silva, L A.(2020). *As criptomoedas e os novos desafios ao sistema monetário: uma abordagem pós-keynesiana.* Economia e Sociedade dez. 2020, Volume 29 N. 3 Pages 761 - 778. [Na Internet]. Disponível em: <https://doi.org/10.1590/1982-3533.2020v29n3art04>. [Consultado em 10/11/2021].

Merkle, R. C.(1978). *Secure communications over insecure channels.* Communications of the ACM, Vol. 21, No. 4 (April 2078), 294-299.

Merkle, R. C.(1979). *Secrecy, authentication, and public-key systems.* PhD. Thesis, Stanford University (1979).

Merkle, R. C.(1982). *Method of providing digital signatures.* [Na Internet]. Disponível em: <https://patentimages.storage.googleapis.com/69/ab/d9/2ff9f94fada6ea/US4309569.pdf >. [Consultado em 14/12/2022].

Monero Project.(2017). [Na Internet]. Disponível em: <http://www.getmonero.org>. [Consultado em 04/01/2023].

Nakamoto, S.(2008). Bitcoin: A peer-to-peer electronic cash system. [Na Internet]. Disponível em: <http://www.bitcoin.org/ > [Consultado em 12/02/2023].

Nakamoto, S.(2008a). Re: Bitcoin P2P e-cash paper.(November 13, 2008). [Na Internet]. Disponível em: <https://www.mail-archive.com/cryptography@metzdowd.com/msg09997.html>.[Consultado em 12/02/2023].

Nerurkar, P., Patel, D., Busnel, Y., Ludinard, R., Kumari, S. & Khan, M. K.(2021). *Dissecting bitcoin Blockchain: Empirical analysis of bitcoin network(2009–2020),* Journal of Network and Computer Applications, Volume 177, 2021, 102940, ISSN 1084-8045,
https://doi.org/10.1016/j.jnca.2020.102940. [Na Internet]. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1084804520303982>. [Consultado em 28/01/2021].

Nogueira, A., Casimiro, A., Bessani, A.(2017). *Elastic state machine replication.* IEEE Transactions on Parallel and Distributed. Systems 28 (9)(2017) 2486–2499.

Plus500(2022). *What is the difference between Ethereum and Bitcoin?* Revista Plus500. [Na Internet]. Disponível em: <https://www.plus500.com/pt-BR/Instruments/ETHUSD/What-is-the-difference-between-Ethereum-and-Bitcoin~2>. [Consultado em 24/06/2022].

Revoredo, T. (2019). *Blockchain - Tudo que você precisa saber.* São Paulo, The Global Strategy.

Salman, T., Zolanvari, M., Erbad, A., Jain, R. & Samaka, M.(2019). *Security Services Using Blockchains: A State of the Art Survey.* In IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 858-880, First Quarter 2019, doi: 10.1109/COMST.2019.2863956.
[Na Internet]. Disponível em: <https://ieeexplore.ieee.org/abstract/document/8428402>. [Consultado em 18/12/2022].

Schneider, F. B.(1990). *Implementing fault-tolerant services using the state machine approach: A tutorial.* ACM Computing Surveys, Vol. 22, No. 4, (1990), 299–319.

Shamir, A.(1984). *Identity Based Cryptosystems and Signature Scheme.* In G. R. Blakley, and David Chaum (Eds.). Advances in Cryptology - CRYPTO 1984. 196.

Sherman, A. T., Javani, F., Zhang, H. and E. Golaszewski, E.(2019). *On the Origins and Variations of Blockchain Technologies.* in IEEE Security & Privacy, vol. 17, no. 1, pp. 72-77, Jan.-Feb. 2019, doi: 10.1109/MSEC.2019.2893730.

Smart cities market.(2020). *Smart cities market - Growth, thends and forecast (2020 - 2025).*
[Na Internet]. Disponível em:
<https://www:mordorintelligence:com/industryreports/smart-cities-market. [Consultado em 22/12/2022].

Spengler, A. & Souza, P.(2021). *Avaliação de desempenho do Hyperledger Fabric com banco de dados para o armazenamento de grandes volumes de dados médicos.* In *Anais do XX Workshop em Desempenho de Sistemas Computacionais e de Comunicação*, (pp. 61-72). Porto Alegre: SBC. doi:10.5753/wperformance.2021.15723. [Na Internet]. Disponível em:
<https://doi.org/10.5753/wperformance.2021.15723>. [Consultado em 06/11/2021].

Stuart, H. and Stornetta, W. S.(1990). *How to time-stamp a digital document in Advances in Cryptology: Proceedings of Crypto `90.* Menezes and Vanstone, eds., LNCS 537, Springer (1991), 437-455.

Tapscott, D. and Tapscott A.(2016). *Blockchain Revolution - Como a tecnologia por trás do Bitcoin está mudando o dinheiro, os negócios e o mundo.* São Paulo, SENAI-SP.

Wust, K. & Gervais, A.(Jun. 2018). *Do you need a Blockchain?* in Proc. Crypto Valley Conf. Blockchain Technol.(CVCBT), pp. 45–54.

Zheng, Z., Xie, S., Dai, H. N., and Wang, H.(2016). *Blockchain challenges and opportunities: A survey.* Work Pap.