12º Congresso Brasileiro de Engenharia de Fabricação
10 a 12 de maio de 2023, Brasília, DF, Brasil

BLOCKCHAIN NA INDÚSTRIA 4.0 - DEFINIÇÃO, APLICABILIDADE E DESENVOLVIMENTO

Gabriel Arão [1]
Jones Yudi [2]
Grupo de Automação e Controle, Universidade de Brasília
[1] gabriel.arao@aluno.unb.br, [2] jonesyudi@unb.br

Resumo: *Indústria 4.0 é um termo que se refere à adoção de diversas tecnologias emergentes e novos paradigmas em diversos setores da indústria como Internet das Coisas, Inteligência Artificial, Sistemas Ciber Físicos, Virtualização, entre outros. Essa nova revolução industrial garante maior automação, produtividade, qualidade, confiabilidade, segurança e eficiência quando comparado com o modelo tradicional, chamado de Indústria 3.0. Nos últimos anos, Blockchain chamou atenção pelo seu uso bem-sucedido em criptomoedas, demonstrando sua capacidade em criar sistemas de registros descentralizados e seguros. As suas características de segurança e eficiência, sua concepção baseada em tecnologias já conhecidas, e a relativa simplicidade da ideia garantem aplicabilidade nos mais diversos contextos e motivaram a rápida evolução da tecnologia para se adaptar aos requisitos técnicos da Indústria 4.0. Atualmente, Blockchain já é considerada uma das tecnologias habilitadoras da revolução que é a Indústria 4.0, conferindo maior transparência e rastreabilidade nos processos industriais, maior nível de automação e facilidade no gerenciamento de redes de Internet das Coisas, além de fornecer maior privacidade e governança sobre os dados, facilitando a construção de ecossistemas colaborativos e descentralizados, essenciais para se garantir a rápida adaptabilidade da indústria em um mundo globalmente conectado com mudanças rápidas e constantes. Além disso, o conceito de tokenização existente em Blockchain condiz com o conceito de sistemas ciber físicos da Indústria 4.0, podendo ser naturalmente aplicado para melhorar o rastreamento de bens e o acompanhamento do ciclo de vida de produtos e maquinário. O presente artigo de revisão visa apresentar em detalhes o que é Blockchain, a evolução da tecnologia desde a sua concepção, incluindo os tipos de Blockchain, uma representação de sua arquitetura geral em camadas, estrutura de dados básica e as principais soluções comerciais disponíveis. Além disso, é apresentado o estado da arte em termos de aplicações de Blockchain na Indústria 4.0, que incluem o gerenciamento e segurança de dispositivos de Internet das Coisas Industrial, armazenamento e compartilhamento de dados e aplicações na indústria como cadeia de suprimentos e Smart Grid, sendo discutidas também as principais vertentes de pesquisa e desenvolvimento, evidenciando os principais problemas e desafios em aberto atualmente que devem ser superados para garantir a evolução e popularização da tecnologia. Por fim, é apresentada a tendência de adoção da tecnologia na Indústria, a começar pelos registros de transições em cadeias de suprimentos, que se justifica pelos grandes benefícios que podem ser obtidos.*

Palavras-chave: *Blockchain; Indústria 4.0; IIoT; Cibersegurança*

1. INTRODUÇÃO

Os vários setores da indústria estão em constante desenvolvimento e evolução, a mais recente delas sendo representada pelo termo Indústria 4.0, que é marcada pela maior conectividade da hierarquia industrial e pela digitalização de processos, garantindo maior velocidade na transmissão dos dados, mais eficiência nos processos e celeridade na tomada de decisão, além do volume sem precedentes de dados gerados e armazenados que possibilitam análises e previsões que, por si mesmos, constituem uma nova área de especialização. A alta conectividade de sensores, atuadores e demais dispositivos via internet é conhecida hoje como Internet das Coisas (IoT) ou Internet das Coisas Industrial (IIoT) e tecnologias como armazenamento de dados em Nuvem e modelos de Inteligência Artificial (IA) são de vital importância para a indústria moderna.

Porém, ataques cibernéticos constantes e os custos operacionais envolvidos na realização de um número massivo de transações diárias são dois grandes problemas que o novo modelo da indústria tem que lidar. Blockchain, uma tecnologia que têm chamado atenção nos últimos anos, está agora sendo adotada pela indústria para tentar resolver essas questões. Blockchain consiste em uma tecnologia capaz de registrar transações digitais de maneira segura, eficiente e descentralizada, sendo revolucionária quando comparada com os métodos tradicionais de se realizar registros e transações de dados. Usando Blockchain, a Indústria 4.0 dará mais um passo em direção à um futuro mais sustentável, eficiente e seguro.

Este artigo de revisão tem como objetivo familiarizar o leitor com o que é Blockchain, como ele é aplicável na Indústria 4.0 e qual o atual estágio de desenvolvimento da tecnologia. As principais contribuições deste trabalho são 1) apresentar e definir o que é Blockchain, suas características, evolução, tipos, estrutura de dados, arquitetura e soluções

comerciais, 2) definir as principais aplicações de Blockchain na Indústria 4.0 e 3) discutir os principais desafios para adoção de Blockchain na Indústria 4.0 e fornecer um contexto do estágio atual do desenvolvimento da tecnologia. O artigo está estruturado da seguinte forma: na Seção 2 são apresentados outros trabalhos de revisão relacionados. Na Seção 3 é definido o que é Blockchain e os principais pontos para entendimento da tecnologia. As seções 4 e 5 discutem as principais aplicações e desafios para Blockchain na Indústria 4.0, respectivamente. Por fim, a Seção 6 conclui o artigo.

2. TRABALHOS RELACIONADOS

Com a crescente relevância do tema, diversos trabalhos de revisão podem ser encontrados nos anos recentes. A Tabela 1 resume os principais trabalhos de revisão considerados.

Tabela 1. Relação de trabalhos relacionados

Referência	Foco
Alladi *et al.* (2019)	Análise dos benefícios e desafios do uso de Blockchain em IIoT por caso de uso.
Aceto *et al.* (2019)	Discussão acerca das tecnologias habilitadoras da Indústria 4.0, incluindo Blockchain como a mais recente.
Wang *et al.* (2020b)	Aplicações e desafios do uso de Blockchain em IoT e IIoT.
Sengupta *et al.* (2020)	Ataques, vulnerabilidades e soluções usando Blockchain em IoT e IIoT.
Zhang e Chen (2020)	Tendências e pesquisas em IoT, Blockchain, Indústria 4.0 e Business Analytics.
Perera *et al.* (2020)	Discussão sobre os riscos, benefícios e a aplicabilidade de Blockchain para a construção civil.
Zuo (2021)	Aplicações e novos modelos de negócio com o uso de Blockchain em IoT, principalmente em manufatura inteligente.
Zheng *et al.* (2021)	Revisão sistemática acerca da aplicabilidade de tecnologias habilitadoras da Indústria 4.0, incluindo Blockchain.
Hameed *et al.* (2022)	Análise aprofundada da taxonomia do Blockchain e discussão sobre o requisitos técnicos e segurança de adotá-lo na Industria 4.0.
Joshi *et al.* (2022)	Benefícios e dificuldades na adoção de Blockchain para segurança e privacidade no contexto da Indústria 4.0.
Huo *et al.* (2022)	Apresenta um método de realização de pesquisas na área, além de comparar as principais plataformas disponíveis no mercado para uso de Blockchain.
Pérez *et al.* (2022)	Discute as vantagens e cria um framework para aplicar Blockchain em modelos de negócio baseados em customização em massa.

Aceto *et al.* (2019) e Zheng *et al.* (2021) colocam a Indústria 4.0 sob a perspectiva de suas tecnologias habilitadoras, incluindo Blockchain como uma das tecnologias mais recentes e disruptivas. A partir dessa perspectiva é possível descobrir como Blockchain se encaixa no cenário mais amplo da Indústria 4.0. Segundo Aceto *et al.* (2019), as características inerentes do Blockchain fazem com que seja uma solução quase ideal para suprir os muitos requisitos da visão colaborativa na Indústria 4.0, especialmente no que se refere à segurança da integração horizontal e ponta a ponta. Zheng *et al.* (2021) destacam o uso de de Blockchain para rastreamento de materiais e acompanhamento do ciclo de vida de produtos inteligentes.

Perera *et al.* (2020), Hameed *et al.* (2022) e Huo *et al.* (2022) se aprofundam na estrutura de dados, taxonomia, topologia de rede, funcionamento e evolução do Blockchain, deixando clara a rápida evolução da tecnologia e os principais desafios enfrentados, além das diversas soluções atualmente sob desenvolvimento. Perera *et al.* (2020) focam na discussão da aplicabilidade de Blockchain na construção civil e discute o conceito, arquitetura, interpretação e casos de uso do Blockchain, bem como perspectivas futuras. Hameed *et al.* (2022) apresentam as características, evolução, tipos e arquitetura em camadas do Blockchain, discutindo também os requisitos de segurança na Indústria 4.0 e como Blockchain se encaixa para suprir essas necessidades, ao mesmo tempo que apontam as questões de segurança não cobertas pela tecnologia. Huo *et al.* (2022) apresentam uma definição e arquitetura em camadas do Blockchain, citando as principais aplicações e fornecendo um método para pesquisa em Blockchain focado em suprir as demandas de cada camada da arquitetura.

Já Alladi *et al.* (2019), Wang *et al.* (2020b), Zuo (2021) e Pérez *et al.* (2022) focam na aplicação prática da tecnologia no contexto da Indústria 4.0, considerando diversos setores da indústria. São apresentados benefícios, desafios e perspectivas futuras, incluindo novos modelos de negócio que podem surgir com o uso de Blockchain. Alladi *et al.* (2019) apontam o uso de Blockchain no contexto de saúde e farmácia, logística, energia, e cadeia de suprimentos, enquanto que Wang *et al.* (2020b) discutem seu uso em Smart Cities, Smart Homes, Big data, veículos elétricos, entre outros. Zuo (2021) trás uma extensa explicação do que é Blockchain, benefícios e desafios de adoção na Indústria 4.0, discutindo seu uso na cadeia de suprimentos, manufatura robotizada, manufatura aditiva, Edge Computing e no setor elétrico. Por fim, Pérez *et al.* (2022) focam no uso de Blockchain para dar suporte à customização em massa na indústria de manufatura.

Focando nos temas de segurança e privacidade, Sengupta *et al.* (2020) discutem ataques e vulnerabilidades em IoT, ao mesmo tempo que listam soluções que se baseiam em Blockchain. Joshi *et al.* (2022) focam na discussão sobre benefícios e dificuldades da adoção de Blockchain para privacidade e segurança na Indústria 4.0. Por fim, Zhang e Chen (2020) compilam diversas pesquisas e tendências considerando Blockchain, IoT, Indústria 4.0 e Business Analytics.

3. DEFINIÇÃO DE BLOCKCHAIN

Blockchain é um mecanismo para registro de informações de maneira descentralizada, segura e auditável. A ideia central do Blockchain é armazenar registros de transações, seja de bens materiais ou imateriais, sem a necessidade de um intermediador ou autoridade central, o que resulta em um sistema mais eficiente e sem um ponto único de falha. Além disso, a estrutura de dados e o modo de operação garantem registros corretos, imutáveis e auditáveis, evidenciando qualquer tentativa de fraude ou golpe. A sua natureza descentralizada também o tornam a ferramenta ideal para registros de transações entre organizações, acabando com a necessidade de se manter registros particulares e paralelos sobre as mesmas transações.

Proposto inicialmente por Nakamoto (2008) no lançamento da criptomoeda Bitcoin, o termo Blockchain não foi usado inicialmente, só se popularizando mais tarde (Johnsen, 2020). Apesar de não mencioná-lo nominalmente, o sistema proposto no Bitcoin usa Blockchain com o conceito de tokenização, onde cada token é atribuído a um cliente, podendo ser transferido para outros. Todas as transações são públicas, checadas e registradas pelos demais clientes da rede, possuindo características de segurança que faz com que muitas pessoas confiem e adotem o Bitcoin como unidade monetária.

Desde o lançamento do Bitcoin e a popularização das criptomoedas, Blockchain já evolui e se modificou o suficiente para ser aplicável em diversos contextos. Um dos marcos mais importantes da tecnologia foi a criação de Smart Contracts pela plataforma Etherum, que são programas armazenados na estrutura de dados do Blockchain, e que são automaticamente executados quando as condições do contrato são atendidas, sem nenhuma entidade reguladora central.

Esta seção se dedica a apresentar os detalhes de funcionamento do Blockchain, se aprofundando nos aspectos mais importantes e dando ao leitor o conhecimento necessário para compreender seus princípios de segurança e características. A Seção 3.1 apresenta a arquitetura de camadas do Blockchain, explicando-as individualmente, na Seção 3.2 algumas das principais características do Blockchain são apresentadas, além de fornecer uma perspectiva histórica da evolução do Blockchain e, por fim, a Seção 3.3 apresenta algumas das soluções comerciais mais conhecidas, além de fornecer um guia para a escolha correta de uma solução usando Blockchain.

3.1. Arquitetura em camadas

Huo *et al.* (2022), Hameed *et al.* (2022) e Perera *et al.* (2020) apresentam representações em camadas da arquitetura de Blockchain, que pode ser resumida na arquitetura de cinco camadas mostrada na Fig. 1. Na arquitetura em camadas, é comum que cada camada possua uma interface de comunicação com as camadas acima e abaixo, com limites bem definidos. Entretanto, em uma arquitetura descentralizada, algumas camadas são mais abstratas e servem mais para facilitar o entendimento.

Figura 1. Arquitetura em camadas em Blockchain

3.1.1. Camada de dados

A estrutura de dados do Blockchain, conforme apresentada por Nakamoto (2008) e representada na Fig. 2, é feita para garantir a integridade das informações gravadas, facilitando a verificação dos blocos e suas transações. Ela consiste em uma cadeia de blocos, onde o bloco seguinte aponta e comprova a autenticidade do anterior através de uma função hash. As informações gravadas no corpo do bloco tem sua autenticidade comprovada através do uso de uma Árvore de Merkle (Merkle, 1989).

Na Figura 2 estão visíveis o cabeçalho e o corpo da estrutura, de maneira simplificada. Cada bloco possui o hash do bloco anterior em seu cabeçalho, com exceção do primeiro bloco, chamado de bloco gênese (Perera *et al.*, 2020). Além disso, um valor aleatório (*Nonce*) é usado em alguns algoritmos de consenso para manipular o resultado do hash do bloco atual, como o *Proof of Work* (PoW).

Considerando um contexto de transação entre duas partes, seja de um bem material ou digital, a transação deve ser assinada digitalmente por ambas as partes envolvidas usando suas chaves criptográficas privadas e verificadas pelos demais

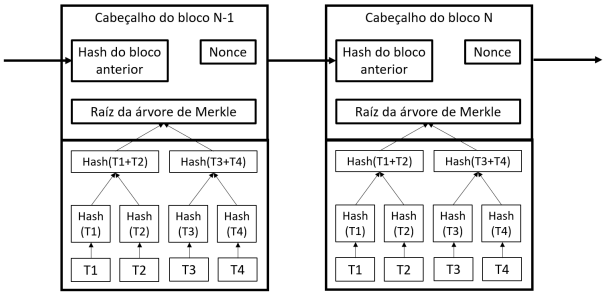

Figura 2. Estrutura de dados básica em Blockchain

clientes da rede através de suas chaves públicas, garantindo a autenticidade e não repúdio da transação. As transações T1 a T4, representadas na figura, fazem parte de uma árvore binária conhecida como Árvore de Merkle, que facilita a verificação da integridade dos dados, além de aliviar o volume de dados armazenados em nós com menor capacidade, que podem armazenar somente os cabeçalhos e solicitar as transações quando necessário. Apesar da figura, mais que quatro transações podem ser gravadas em um único bloco.

Além disso, é importante mencionar que existem dois modelos de armazenamento de dados em aplicações Blockchain, que podem levar a modificações na sua estrutura base. São eles:

- **Armazenamento *On-Chain*:** Os dados são armazenados no próprio Blockchain, seguindo a estrutura tradicional apresentada. Nesse modelo os dados gravados são visíveis para todos na rede e pode exigir maior espaço de armazenamento dos dispositivos e maior latência na rede.
- **Armazenamento *Off-Chain*:** Os dados são armazenados fora do Blockchain, que mantém apenas os valores hash desses dados, para verificação de integridade. Esse modelo garante a privacidade dos dados, além de exigir menor capacidade de armazenamento e reduzir a latência na rede, porém aumentando a complexidade da solução e fazendo com que os dados não compartilhem das características de segurança do Blockchain.

3.1.2. Camada de rede

Na rede Blockchain, os clientes se comunicam diretamente uns com os outros através de protocolos P2P e de broadcast, sem intermediação. A rede Blockchain pode ser permissionada ou não, ou seja, os dispositivos participantes da rede podem ser dispositivos registrados, autenticados e gerenciados por uma ou mais organizações ou podem ser dispositivos anônimos em uma rede aberta. Dado essa característica de permissionamento, os tipos de rede Blockchain são:

- **Blockchain Público:** É a concepção original do Blockchain, consiste em uma rede pública, sem permissionamento, onde os nós da rede podem entrar e sair quando desejarem. Tem como característica o uso de mecanismos de recompensa e punição, para incentivar o bom comportamento dos clientes.
- **Blockchain Privado:** Rede permissionada gerida por uma única organização. Normalmente são redes consideravelmente menores do que as públicas e que buscam maior eficiência e segurança contra atacantes mesmo que isso resulte no aumento de complexidade, hierarquização e menor grau de descentralização na rede.
- **Blockchain Consórcio:** Rede permissionada gerida por mais de uma organização, visando cooperação entre as partes, como em uma cadeia de suprimentos por exemplo. Deve lidar com as complexidades de autenticação e registro com múltiplos gestores, algumas vezes consistindo em várias redes Blockchain privadas menores.
- **Blockchain Híbrido:** Rede parcialmente permissionada, sendo um híbrido entre público e privado. São redes geridas por uma ou mais organizações e que permitem a participação de dispositivos não autenticados e sem privilégios de acesso, normalmente sendo capazes de excluí-los da rede caso necessário.

Com relação à estrutura de rede, ela pode ser **não estruturada**, que é a arquitetura mais tradicional, ou **estruturada**, que torna a rede mais complexa porém melhora a taxa de transmissão de dados consideravelmente, sendo aplicável principalmente para redes privadas. De maneira geral e independente do tipo e estrutura da rede, o comportamento básico da rede Blockchain é o seguinte:

1. Ao se realizar uma transação entre dois clientes, uma nova transação é gerada e assinada pelas partes, usando suas chaves privadas.
2. A transação é transmitida por toda a rede por protocolos P2P, chegando ao máximo de clientes possível.
3. Os demais clientes da rede verificam a validade da transação usando as chaves criptográficas públicas dos envolvidos e verificando o histórico de posse do bem em transição e, caso sejam válidos, demonstram sua aceitação incluindo a transação em um bloco de transações.

4. Os clientes realizam um trabalho, especificado pelo mecanismo de consenso, para incluir o novo bloco de transações verificadas na cadeia de blocos do Blockchain.

5. Quando finaliza o trabalho de inclusão do novo bloco, a nova cadeia de blocos é transmitida pela rede e os demais clientes atualizam seus registros.

Os nós da rede sempre consideram a cadeia mais longa como sendo a mais correta. Em caso de empate, as cadeias de tamanhos iguais são mantidas até que haja um desempate. As mensagens não precisam chegar a todos os nós, contanto que chegue para a maioria, garantindo uma alta tolerância à falhas.

3.1.3. Camada de consenso

Essa camada se refere aos algoritmos de consenso usado para a inclusão de novos blocos na cadeia de blocos, além dos mecanismos de recompensa e punição usados para incentivar o bom comportamento dos clientes em redes públicas. O mecanismo de consenso mais notório, usado pelo Bitcoin e outras criptomoedas, é o *Proof of Work* (PoW). O funcionamento básico do mecanismo PoW consiste em, dado um bloco de transações como o da Fig. 2, incrementar o valor do *Nonce* até que o hash do bloco se inicie com N bits zeros, onde N é um parâmetro ajustável pela rede para controlar o número de novos blocos criados por hora Nakamoto (2008). A lógica de tal mecanismo é de que, como este é um trabalho que requer energia e poder computacional, atacantes não são capazes de criar blocos no mesmo ritmo da rede, de forma que a cadeia mais longa e aceita pelos demais clientes continua sendo a cadeia de blocos honesta. Além disso, a energia e trabalho computacional do atacante é mais bem recompensado trabalhando a favor da rede, validando as transações da criptomoeda, garantindo maior segurança para a rede e gerando moedas para si próprio como recompensa.

Apesar de ser amplamente conhecido e usado, o mecanismo PoW é energeticamente intenso e muito dispendioso, não sendo sustentável a longo prazo em uma escala global, de forma que outros mecanismos similares foram criados como o *Proof of Stake* (PoS), onde os blocos são avaliados por grupos de clientes que 'apostam' criptomoedas na validade do novo bloco e são recompensados caso o o grupo avalie o bloco como válido, criando uma lógica de risco e recompensa similar ao PoW porém com muito mais eficiência de tempo e energia.

Existem também outros tipos de mecanismos de consenso, mais apropriados para serem usados em Blockchains não públicos, que não necessitam de mecanismos de recompensa mas que devem garantir maior segurança, privacidade e eficiência na validação e criação de blocos. Os mecanismos de consenso como um todo podem ser divididos em três categorias:

1. **PoX (Proof of X)** são mecanismos que exigem que os clientes se comprometam com recursos próprios a favor da rede, de forma que um atacante pode perder ou desperdiçar esses recursos caso o restante da rede não concorde com seu comportamento, enquanto que clientes honestos são recompensados. É idealmente usado em redes públicas por contarem com mecanismo de recompensa que incentiva o bom comportamento dos clientes na rede. Incluem algoritmos como PoW, PoS, *Proof of Authority* (PoA), *Proof of Elapsed Time* (PoET), entre tantos outros.

2. **BFT (Bizantine Fault Tolerance):** são inspirados no Problema dos Generais Bizantinos, da Teoria dos Jogos (Huo *et al.*, 2022), em que os generais devem chegar a um acordo quanto à estratégia de ataque a ser usada, mesmo que alguns dos generais sejam inimigos infiltrados. Contanto que os inimigos estejam em minoria, esses algoritmos são capazes de alcançar o consenso.

   Esses mecanismos não possuem uma lógica de incentivo e são mais utilizados em redes privadas, em ambientes controlados, com menos nós na rede e onde se assume que a maioria dos dispositivos sejam honestos e funcionando corretamente. O algoritmo mais conhecido é o Pratical Bizantine Fault Tolerance (PBFT).

3. **CFT (Crash Fault Tolerance)**: são mecanismos focados na resiliência da rede, sendo capazes de alcançar consenso mesmo quando parte da rede está comprometida. Os algoritmos mais conhecidos incluem Paxos, Raft e Kafka (Huo *et al.*, 2022).

3.1.4. Camadas de controle e aplicação

Essas camadas representam lógicas de mais alto nível e que dependem fortemente do tipo de Blockchain e aplicação em que está sendo usado. A camada de controle representa a programação do Blockchain e dita como se dá o processamento e verificação de dados, a consulta de dados no modelo *Off-Chain* e demais lógicas de alto nível, normalmente especializadas para o caso de uso. Essa camada também é responsável pela execução de Smart Contracts, que são uma espécie de contrato digital que, dadas certas condições, executam uma ou mais ações. Por exemplo, uma transação de criptomoedas pode ser condicionada pela detecção de uma tag em um determinado local.

No mais alto nível, a camada de aplicação contém a interface com o usuário, e se comunica com a camada de controle, fazendo consultas, criando novos contratos, realizando transações, cadastrando ou removendo dispositivos, entre outras operações que se disponibilize ao usuário ou programador da solução.

3.2. Características e evolução do Blockchain

Algumas das características de segurança do Blockchain que fazem com que essa seja uma tecnologia tão atrativa são:

- **Descentralização:** A descentralização de sistemas de informação trazem diversos benefícios. O fato da informação estar armazenada em vários dispositivos faz com que o sistema seja redundante, resiliente a falhas e menos propenso a ataques cibernéticos comuns em redes centralizadas.
- **Imutabilidade:** Uma tentativa de alterar registros passados é frustrada pois, devido ao fato dos registros serem distribuídos entre todos os nós da rede, essa ação precisa passar pelo mecanismo de consenso para ser verificado e aprovado por todos os demais participantes. Além disso, a estrutura de dados adotada em Blockchain faz com que todo o histórico de informações possa ser rapidamente checado, de forma que a menor alteração é imediatamente percebida.
- **Não repúdio:** Blockchain exige que todo registro seja assinado digitalmente pelo dispositivo emissor da informação. Quando em um contexto de tokenização, é inegável afirmar que os dois nós realizaram uma transação, devido à presença das assinaturas de ambas as partes.
- **Transparência/Auditabilidade:** Na rede descentralizada criada via Blockchain, todos os nós da rede compartilham as tarefas de verificação e armazenamento dos registros e transações, de forma que essas informações são públicas e auditáveis para os participantes da rede.
- **Anonimidade:** A rede possui identificadores internos (como número da carteira, no caso de criptomoedas), de forma que os integrantes da rede não precisam compartilhar informações acerca de si mesmos para participarem. Ainda assim, devido à publicidade dos registros e a existência de informação externa, é possível quebrar a anonimidade de pessoas em alguns casos, sendo necessário o uso de outras técnicas caso se deseje garantir a anonimidade.
- **Autonomia da rede**: Uma rede descentralizada que usa Blockchain e Smart Contracts é capaz de operar de forma autônoma, emitindo, verificando e armazenando transações e demais informações automaticamente.

Alguns autores como Hameed *et al.* (2022) e Ahmed *et al.* (2022) dividem a evolução do Blockchain em cinco momentos, representados na Fig. 3. As características mais marcantes de cada fase são descritas a seguir:

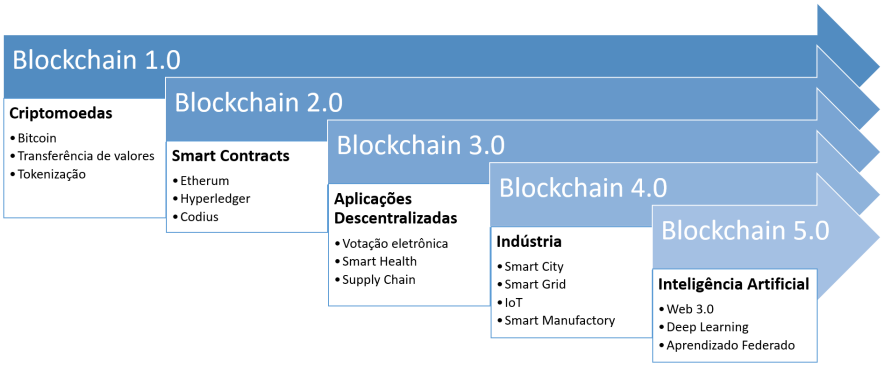

Figura 3. Evolução do Blockchain

1. **Blockchain 1.0 - Criptomoedas:** Inaugurando as aplicações Blockchain estão o Bitcoin e demais criptomoedas. Blockchain é usado com o conceito de tokens digitais e transferência de valores.
2. **Blockchain 2.0 - Smart Contracts:** A primeira evolução que marcou Blockchain foi a concepção de Smart Contracts pela plataforma Etherum. Smart Contracts são programas auto executáveis gravados no Blockchain, permitindo a automação de tarefas, e são a base para as próximas evoluções.
3. **Blockchain 3.0 - Aplicações Descentralizadas:** Conforme Blockchain passou a ser utilizado em contextos como cadeia de suprimentos e Smart Health, o volume de dados passou a ser um problema. A terceira evolução da tecnologia visou aplicar Blockchain para descentralizar o trabalho realizado por servidores, com alta capacidade de armazenamento, e a criação de aplicações descentralizadas mais seguras. Uma das grandes vantagens dessa evolução foi a possibilidade dos programadores usarem qualquer linguagem de programação para desenvolvimento dessas soluções.
4. **Blockchain 4.0 - Indústria:** Conforme Blockchain e Indústria 4.0 convergem, Blockchain precisou evoluir para acompanhar e suprir as demandas dos diversos cenários Industriais. Não apenas requisitos de armazenamento como também segurança, privacidade, escalabilidade e taxa de transmissão de dados são prioridades nessa fase da evolução.

5. **Blockchain 5.0 - Inteligência Artificial:** A mais recente evolução diz respeito à descentralização da Web e de técnicas de Inteligência Artificial (IA). Com Blockchain preparado para ser aplicado em contextos reais, o enorme volume de dados pode ser usado para construção de modelos inteligentes de maneira descentralizada, colaborativa e segura, mantendo a privacidade e propriedade dos dados.

3.3. Soluções comerciais

Atualmente existe uma gama de opções de plataformas Blockchain para se escolher, para os mais diversos cenários e aplicações. Os critérios que organizações devem considerar para realizar a escolha de uma plataforma específica incluem custo, mecanismo de consenso, suporte a Smart Contracts, performance, ferramentas de desenvolvimento disponíveis, maturidade da plataforma, entre outros. Huo *et al.* (2022) e Perera *et al.* (2020) analisam as características das plataformas Blockchain mais populares, que incluem Etherum, IBM Blockchain, Hyperledger Fabric, Hyperledger Sawtooth, Azure Blockchain, entre outros.

De forma geral, a escolha da plataforma de Blockchain ideal envolve o trilema representado na Fig. 4, onde não é possível atender todos os requisitos de segurança, descentralização e escalabilidade simultaneamente (Perera *et al.*, 2020; Huo *et al.*, 2022). A segurança, considerado um dos pilares e motivos para adoção do Blockchain, é garantido pelas principais plataformas comerciais, que então escolhem atender aplicações que exigem mais escalabilidade ou descentralização.

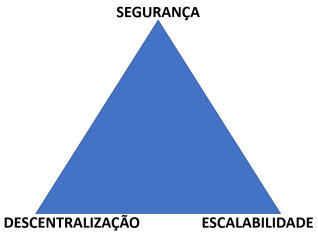

Figura 4. Trilema do desenvolvimento em Blockchain

A relação de oposição entre escalabilidade e descentralização vêm do fato de que, quanto maior a rede, maior será a latência de comunicação para que todos participem do processo de consenso, principalmente em mecanismos BFT tipicamente usados em redes privadas, fazendo com que compense abrir mão da descentralização concentrar mais poder de decisão em alguns nós de uma rede estruturada em prol de maior escalabilidade da rede. Por outro lado, a ideia de concentrar maior poder em alguns clientes em redes Blockchain públicas como o Bitcoin é impensável e perigoso, de forma que a rede deve se apoiar na descentralização total como forma de proteção, sacrificando a escalabilidade e eficiência no processo.

4. APLICAÇÕES DE BLOCKCHAIN NA INDÚSTRIA 4.0

As aplicações de Blockchain na Indústria 4.0 podem ser divididas em três vertentes principais (Huo *et al.*, 2022):

1. **Gerenciamento e segurança de dispositivos:** são aplicações que usam Blockchain para cadastro e autenticação de dispositivos, unificando o padrão de gerenciamento mesmo com a heterogeneidade de dispositivos IoT e explorando as vantagens oferecidas pela descentralização;

2. **Armazenamento e compartilhamento de dados:** usam Blockchain para criar uma camada de controle de acesso aos dados que promove mais privacidade e facilita o gerenciamento e compartilhamento de informações dentro de uma organização ou em um contexto mais amplo, envolvendo múltiplas organizações.

3. **Aplicações Industriais:** adaptam as soluções e aplicam a um caso de uso real, usando Blockchain para rastrear matéria-prima, produtos e operações industriais através do conceito de tokenização, regulam trocas energéticas ou o processo de Aprendizado de Máquina distribuído, entre outras aplicações.

A seguir são apresentados os principais e mais recentes avanços em aplicações nessas três áreas.

4.1. Gerenciamento e segurança de dispositivos

De maneira geral, redes IIoT devem adotar sistemas para gerenciamento e autenticação dos dispositivos da rede. Os principais desafios enfrentados por tais sistemas estão relacionados à proteção das chaves criptográficas, a privacidade dos dados e a rastreabilidade da atividade dos dispositivos na rede, além da detecção automática de falhas e ataques que devem desencadear medidas que visam mitigar possíveis danos. Além disso, redes IIoT muitas vezes são heterogêneas e os sistemas de gerenciamento devem fornecer um certo nível de padronização no cadastro e gerenciamento desses dispositivos.

De forma geral, Blockchain pode fornecer uma estrutura segura que oferece imutabilidade, não repúdio, que facilita a detecção de anomalias e com suporte para redes heterogêneas para registrar informações que, em conjunto com outras

técnicas criptográficas, pode oferecer a privacidade e confidencialidade necessárias para tais sistemas. Além disso, tarefas rotineiras e o registro de atividades podem ser automatizadas através de Smart Contracts.

Wang *et al.* (2021) propõem um sistema baseado em Blockchain e Smart Contracts para autenticação de dispositivos IIoT sem Certificado Digital. O esquema descentraliza o processo de geração de chaves, considerado um risco de segurança em outros sistemas de autenticação similares, tornando a rede mais resistente a ataques como *Man-in-the-Middle* (MitM).

Latif *et al.* (2021) demonstram o uso de Blockchain em uma planta de processamento de frutas, usando Blockchain privado e Smart Contracts para criar uma camada de registro e autenticação de usuários e dispositivos IIoT, além de transmitir comandos aos atuadores e armazenar dados da operação.

Li *et al.* (2022) propõem um protocolo AGKA (Assimetric Group Key Agreement) para lidar com a segurança das chaves criptográficas usando Blockchain, o que garante a automação do controle de acesso usando Smart Contracts, além das características de imutabilidade e não repúdio do Blockchain.

4.2. Armazenamento e compartilhamento de dados

Em aplicações IoT é comum haver um grande volume de dados que devem ser armazenados e compartilhados com terceiros de maneira segura. O sistema ideal para compartilhamento deve ter uma certa granularidade de permissões para possibilitar compartilhamento somente aos dados necessários e nenhum outro, além de oferecer rastreabilidade dos acessos realizados e a facilidade de gerenciar e revogar os acessos quando necessário.

Blockchain pode ser usado para se criar uma camada intermediária entre os dados e os usuários, verificando permissões e registrando todos os acessos realizados de maneira transparente e rastreável. A descentralização da solução facilita a criação de cenários colaborativos entre organizações que desejam compartilhar dados de maneira segura e controlada.

Gai *et al.* (2020) propõem uma combinação de Blockchain e Edge Computing, usando técnicas de Privacidade Diferencial para garantir a privacidade de dados sobre alocação de tarefas. O sistema garante eficiência energética, segurança e governança dos dados privados dos usuários.

Tian *et al.* (2021) propõem o BML-ES, um framework para uso de Machine Learning (ML) em IIoT baseado em Blockchain. Baseado no conceito de Federated Learning, o framework propõe uma estratégia para agregar os modelos de ML locais para obtenção de um modelo global, bem como o uso de Smart Contracts como mecanismo de incentivo para a participação dos nós na rede.

Rahman *et al.* (2021) desenvolvem um sistema Blockchain com armazenamento híbrido *on-chain* e *off-chain* na nuvem para eficiência em dispositivos IIoT, além de um método criptográfico para preservar a privacidade dos dados armazenados ao mesmo tempo que permite o compartilhamento e a rapidez nas consultas aos dados.

Qi *et al.* (2020) propõem o Cpds, um sistema voltado para armazenamento eficiente e compartilhamento de dados descentralizado e unificado para IIoT. Baseado em Blockchain, o sistema permite que múltiplas organizações gerenciem acesso e compartilhem dados de maneira segura, ao mesmo tempo que garante a eficiência de armazenamento usando técnicas de compressão de dados.

Gao *et al.* (2020) consideram os riscos de segurança e privacidade em Pervasive Edge Computing (PEC) e Software-Defined Networks (SDN), dois paradigmas emergentes em IIoT, e propõe o uso de Blockchain e Proxy Reencryption para permitir o compartilhamento seguro de dados entre dispositivos, bem como reduzir riscos de segurança provenientes da arquitetura centralizada. Smart Contracts também são usados para busca e atualização de registros em Blockchain.

Yu *et al.* (2021) desenvolvem um sistema para compartilhamento de Smart Factory Big Data (SFBD) com parceiros comerciais baseado em Blockchain. O sistema realiza registro e autenticação de dispositivos e usuários, registrando acessos realizados e sendo capaz de detectar e rastrear anomalias e acessos não autorizados, revogando automaticamente o acesso.

Lu *et al.* (2021) propõem um protocolo baseado em Blockchain para compartilhamento de dados de sensores IIoT armazenados em nuvem. Um novo esquema de assinatura em grupo é desenvolvido e combinado com Smart Contracts e Proxy Reencryption para garantir privacidade, segurança e eficiência.

4.3. Aplicações Industriais

A Indústria 4.0 engloba uma série de setores que podem se beneficiar do uso de Blockchain, como a manufatura, a gestão da cadeia de suprimentos, saúde, energia, veículos autônomos, entre outros. A seguir estão descritos algumas das principais e mais recentes pesquisas nas áreas da indústria cuja aplicação de Blockchain é mais proeminente.

4.3.1. Smart Grid

Um novo termo derivado da Indústria 4.0 e que abarca uma série de tecnologias emergentes é Smart Grid, relacionada com o uso de IoT no setor de energia e que permite um maior controle e rastreabilidade sobre consumo e produção energética. Blockchain é encarado como uma tecnologia promissora para possibilitar trocas energéticas mais seguras e eficientes, de maneira descentralizada e independente.

Li *et al.* (2018) propõem um sistema para troca energética segura baseado em Blockchain de consórcio. Através do uso de Smart Contracts, o sistema garante o cumprimento do acordo entre as partes, automatizando a tarefa e eliminando riscos de transações fraudulentas, além de propor um esquema para determinação de preços de forma dinâmica.

Li *et al.* (2020) apresentam o FeneChain, um sistema baseado em Blockchain que supervisiona e gerencia o processo de troca energética, focado em segurança, privacidade e eficiência. No contexto da Indústria 4.0, o sistema garante a aquisição de energia rastreável e de maneira segura.

Guan *et al.* (2020) apresentam o BC-ETS, um sistema que visa melhorar a eficiência, segurança e escalabilidade de esquemas de troca energética tradicionais. Baseado em Blockchain, o sistema usa um esquema baseado em crédito para se adequar à capacidade computacional de dispositivos IoT.

4.3.2. Machine Learning

O volume de dados gerados em aplicações IoT é perfeito para treinar modelos de ML, que dependem desses dados. Um novo método de treinamento, conhecido como *Federated Learning* (FL) (McMahan *et al.*, 2017) permite que modelos de ML sejam treinados de maneira descentralizada, sem a necessidade de reunir os dados em um servidor, preservando a privacidade dos dados, promovendo mais eficiência nas comunicações da rede e reduzindo custos de armazenamento e manutenção. Porém, FL ainda requer que o poder decisório seja concentrado na figura central de um orquestrador, o que diminui a sua característica descentralizada. O uso de Blockchain unido a FL é visto como uma forma de tornar o método descentralizado de fato, tornando-o ainda mais promissor para uma série de desafios. A principal preocupação envolvida no uso de Blockchain e FL é como preservar a privacidade dos modelos de ML que são enviados pela rede.

Jia *et al.* (2021) reconhecem os benefícios de FL mas apontam para vulnerabilidades e ataques que visam os modelos de ML locais gerados. Para oferecer mais segurança e privacidade, é proposto um sistema para FL baseado em Blockchain que utiliza Privacidade Diferencial e Criptografia Homomórfica para proteger os modelos de ML compartilhados.

Zhang *et al.* (2021) propõem BC-EdgeFL, um modelo de transmissão de dados para FL e Edge Computing baseado em Blockchain. Os experimentos mostram altas taxas de acurácia do modelo e de detecção de informações ilegais, tornando o sistema seguro e eficiente.

4.3.3. Cadeia de Suprimentos

Rastreabilidade e compartilhamento de informações entre organizações parceiras é especialmente relevante na cadeia de suprimentos, sendo um ambiente natural para a aplicação de Blockchain, que permite alcançar um novo nível de segurança e colaboração entre os muitos stakeholders. O uso de Blockchain trás mais transparência e informação acerca da produção, gerando mais inovação, eficiência e confiança de ponta a ponta da cadeia, desde os fornecedores primários até o cliente final.

Sistemas de compartilhamento de dados como os desenvolvidos por Yu *et al.* (2021) e Lu *et al.* (2021) são essenciais para possibilitar uma maior adoção de Blockchain em cadeia de suprimentos. Rashid *et al.* (2022) realizam uma análise aprofundada sobre os impactos da adoção da tecnologia em termos de rastreabilidade, transparência, performance e confiança entre as partes.

Cao *et al.* (2019) propõem um sistema baseado em Blockchain para rastreabilidade de cadeia de suprimentos na indústria metalúrgica, tornando a produção mais transparente e aumentando a rastreabilidade do trabalho realizado. Além disso, o maior nível de automação e informação eleva a eficiência e confiança em toda a cadeia.

5. EVOLUÇÃO E MELHORIAS EM BLOCKCHAIN

Existem diversos desafios que precisam ser vencidos para ampliar a confiança e adoção de Blockchain na Indústria 4.0. Primeiramente, as limitações de armazenamento e processamento dos dispositivos IIoT exige a construção de modelos de armazenamento inovadores, estruturação da rede com separação de responsabilidades, simplificações na estrutura de dados básica, além de mecanismos de consenso energeticamente eficientes.

Muitos contextos industriais também exigem alta escalabilidade, comunicação com baixa latência e alta taxa de transmissão de dados, requisitos que Blockchain ainda sofre para atender. Tentativas de melhorar a escalabilidade, conforme indica o trilema do Blockchain da Fig. 4, acarretam em menor descentralização, que se traduz em hierarquização e divisão de tarefas na rede, fragmentação e distribuição dos dados e o uso de entidades que centralizam algum tipo de poder decisório para orquestração da rede.

Visando remover as limitações de armazenamento e escalabilidade para aplicação de Blockchain em IoT, Yu *et al.* (2020) propõem LayerChain. Através de uma estrutura de rede hierarquizada e clusterização dos nós, LayerChain reduz os requisitos de armazenamento do sistema e os tempos de propagação de blocos, sendo conveniente para aplicações IIoT de larga escala e baixo delay.

Cui *et al.* (2020) propõem o protocolo CoDAG visando melhorar a taxa de transmissão de dados em Blockchain. O protocolo organiza os nós como um Grafo Acíclico Dirigido (DAG na sigla em inglês) compactado, além de realizar simplificações na estrutura de dados. Simulações de ataques são realizadas para demonstrar a segurança do protocolo.

Cai *et al.* (2021) propõem o uso de *Sharding* para distribuição de dados em Blockchain visando melhorias na taxa de transmissão e escalabilidade. Um modelo de otimização multiobjetivo é proposto para definição dos parâmetros.

Cao *et al.* (2020) propõem um modelo de otimização multiobjetivos para definir os parâmetros de uma rede Blockchain privada, visando otimizar escalabilidade, descentralização, latência e custo. O mecanismo de consenso adotado foi PBFT, adequado para redes privadas.

Visando melhorar problemas de segurança presentes em mecanismos de consenso, Wang *et al.* (2020a) propõem PoRX, um esquema de incentivo baseado em crédito que pode ser usado em conjunto com mecanismos PoX e voltado para IIoT. O esquema reforça ainda mais as recompensas e punições, incentivando mais efetivamente o bom comportamento da rede.

6. CONCLUSÃO

Neste artigo de revisão foi apresentada a tecnologia Blockchain e seus possíveis usos na indústria. Espera-se que, com uma definição detalhada e aprofundada, o leitor seja capaz de discernir os benefícios e aplicabilidade dessa tecnologia no contexto da Indústria 4.0, além de perceber os desafios e desenvolvimentos pendentes para que a tecnologia adquira maior robustez e atenda aos requisitos esperados na prática.

Com base no que foi apresentado em termos de evolução, melhorias e vantagens de se utilizar Blockchain, acreditamos que a indústria verá grandes transformações na forma como lida e registra transações, a começar pela gestão da cadeia de suprimentos. Tradicionalmente, ao se realizar a compra e venda de matéria-prima, peças ou outros produtos, cada organização mantém um banco de dados próprio onde se registram todas as transações realizadas. Substituir esse modelo por um modelos descentralizado, altamente automatizável, seguro, transparente e auditável como Blockchain tornará muito fácil a tarefa de rastrear qualquer bem desde a sua origem, reduzirá o volume total de dados digitais armazenados entre as organizações, cortará custos envolvidos no processo, promoverá maior eficiência e dará segurança à Indústria e ao consumidor final quanto à origem do que está sendo consumido. Essa mudança irá exigir a adequação de grande parte dos atores da Indústria e, então, a adoção de Blockchain como mecanismo de registro deve, naturalmente, se alastrar pelas demais áreas das empresas e organizações.

7. REFERÊNCIAS

Aceto, G., Persico, V. e Pescapé, A., 2019. "A survey on information and communication technologies for industry 4.0: State-of-the-art, taxonomies, perspectives, and challenges". *IEEE Communications Surveys & Tutorials*, Vol. 21, No. 4, pp. 3467–3501.

Ahmed, I., Zhang, Y., Jeon, G., Lin, W., Khosravi, M.R. e Qi, L., 2022. "A blockchain-and artificial intelligence-enabled smart iot framework for sustainable city". *International Journal of Intelligent Systems*.

Alladi, T., Chamola, V., Parizi, R.M. e Choo, K.K.R., 2019. "Blockchain applications for industry 4.0 and industrial iot: A review". *IEEE Access*, Vol. 7, pp. 176935–176951.

Cai, X., Geng, S., Zhang, J., Wu, D., Cui, Z., Zhang, W. e Chen, J., 2021. "A sharding scheme-based many-objective optimization algorithm for enhancing security in blockchain-enabled industrial internet of things". *IEEE Transactions on Industrial Informatics*, Vol. 17, No. 11, pp. 7650–7658.

Cao, B., Wang, X., Zhang, W., Song, H. e Lv, Z., 2020. "A many-objective optimization model of industrial internet of things based on private blockchain". *IEEE Network*, Vol. 34, pp. 78–83.

Cao, Y., Jia, F. e Manogaran, G., 2019. "Efficient traceability systems of steel products using blockchain-based industrial internet of things". *IEEE Transactions on Industrial Informatics*, Vol. 16, No. 9, pp. 6004–6012.

Cui, L., Yang, S., Chen, Z., Pan, Y., Xu, M. e Xu, K., 2020. "An efficient and compacted dag-based blockchain protocol for industrial internet of things". *IEEE Transactions on Industrial Informatics*, Vol. 16, pp. 4134–4145.

Gai, K., Wu, Y., Zhu, L., Zhang, Z. e Qiu, M., 2020. "Differential privacy-based blockchain for industrial internet-of-things". *IEEE Transactions on Industrial Informatics*, Vol. 16, pp. 4156–4165.

Gao, Y., Chen, Y., Hu, X., Lin, H., Liu, Y. e Nie, L., 2020. "Blockchain based iiot data sharing framework for sdn-enabled pervasive edge computing". *IEEE Transactions on Industrial Informatics*, Vol. 17, No. 7, pp. 5041–5049.

Guan, Z., Lu, X., Wang, N., Wu, J., Du, X. e Guizani, M., 2020. "Towards secure and efficient energy trading in iiot-enabled energy internet: A blockchain approach". *Future Generation Computer Systems*, Vol. 110, pp. 686–695.

Hameed, K., Barika, M., Garg, S., Amin, M.B. e Kang, B., 2022. "A taxonomy study on securing blockchain-based industrial applications: An overview, application perspectives, requirements, attacks, countermeasures, and open issues". *Journal of Industrial Information Integration*, Vol. 26, p. 100312.

Huo, R., Zeng, S., Wang, Z., Shang, J., Chen, W., Huang, T., Wang, S., Yu, F.R. e Liu, Y., 2022. "A comprehensive survey on blockchain in industrial internet of things: Motivations, research progresses, and future challenges". *IEEE Communications Surveys and Tutorials*, Vol. 24, pp. 88–122.

Jia, B., Zhang, X., Liu, J., Zhang, Y., Huang, K. e Liang, Y., 2021. "Blockchain-enabled federated learning data protection aggregation scheme with differential privacy and homomorphic encryption in iiot". *IEEE Transactions on Industrial Informatics*, Vol. 18, No. 6, pp. 4049–4058.

Johnsen, M., 2020. *Blockchain in Digital Marketing: A New Paradigm of Trust*. Maria Johnsen.

Joshi, S., Pise, A.A., Shrivastava, M., Revathy, C., Kumar, H., Alsetoohy, O. e Akwafo, R., 2022. "Adoption of blockchain technology for privacy and security in the context of industry 4.0". *Wireless Communications and Mobile Computing*, Vol. 2022.

Latif, S., Idrees, Z., Ahmad, J., Zheng, L. e Zou, Z., 2021. "A blockchain-based architecture for secure and trustworthy operations in the industrial internet of things". *Journal of Industrial Information Integration*, Vol. 21.

Li, J., Qiao, Z. e Peng, J., 2022. "Asymmetric group key agreement protocol based on blockchain and attribute for

industrial internet of things". *IEEE Transactions on Industrial Informatics*.

Li, M., Hu, D., Lal, C., Conti, M. e Zhang, Z., 2020. "Blockchain-enabled secure energy trading with verifiable fairness in industrial internet of things". *IEEE Transactions on Industrial Informatics*, Vol. 16, pp. 6564–6574.

Li, Z., Kang, J., Yu, R., Ye, D., Deng, Q. e Zhang, Y., 2018. "Consortium blockchain for secure energy trading in industrial internet of things". *IEEE Transactions on Industrial Informatics*, Vol. 14, pp. 3690–3700.

Lu, J., Shen, J., Vijayakumar, P. e Gupta, B.B., 2021. "Blockchain-based secure data storage protocol for sensors in the industrial internet of things". *IEEE Transactions on Industrial Informatics*, Vol. 18, No. 8, pp. 5422–5431.

McMahan, B., Moore, E., Ramage, D., Hampson, S. e y Arcas, B.A., 2017. "Communication-efficient learning of deep networks from decentralized data". In *Artificial intelligence and statistics*. PMLR, pp. 1273–1282.

Merkle, R.C., 1989. "A certified digital signature". In *Conference on the Theory and Application of Cryptology*. Springer, pp. 218–238.

Nakamoto, S., 2008. "Bitcoin: A peer-to-peer electronic cash system". *Decentralized Business Review*, p. 21260.

Perera, S., Nanayakkara, S., Rodrigo, M., Senaratne, S. e Weinand, R., 2020. "Blockchain technology: Is it hype or real in the construction industry?" *Journal of Industrial Information Integration*, Vol. 17, p. 100125.

Pérez, A.T.E., Rossit, D.A., Tohmé, F. e Óscar C. Vásquez, 2022. "Mass customized/personalized manufacturing in industry 4.0 and blockchain: Research challenges, main problems, and the design of an information architecture". *Information Fusion*, Vol. 79, pp. 44–57.

Qi, S., Lu, Y., Zheng, Y., Li, Y. e Chen, X., 2020. "Cpds: Enabling compressed and private data sharing for industrial internet of things over blockchain". *IEEE Transactions on Industrial Informatics*, Vol. 17, No. 4, pp. 2376–2387.

Rahman, M.S., Khalil, I., Moustafa, N., Kalapaaking, A.P. e Bouras, A., 2021. "A blockchain-enabled privacy-preserving verifiable query framework for securing cloud-assisted industrial internet of things systems". *IEEE Transactions on Industrial Informatics*, Vol. 18, No. 7, pp. 5007–5017.

Rashid, A., Ali, S.B., Rasheed, R., Amirah, N.A. e Ngah, A.H., 2022. "A paradigm of blockchain and supply chain performance: a mediated model using structural equation modeling". *Kybernetes*.

Sengupta, J., Ruj, S. e Bit, S.D., 2020. "A comprehensive survey on attacks, security issues and blockchain solutions for iot and iiot". *Journal of Network and Computer Applications*, Vol. 149, p. 102481.

Tian, Y., Li, T., Xiong, J., Bhuiyan, M.Z.A., Ma, J. e Peng, C., 2021. "A blockchain-based machine learning framework for edge services in iiot". *IEEE Transactions on Industrial Informatics*, Vol. 18, No. 3, pp. 1918–1929.

Wang, E.K., Liang, Z., Chen, C.M., Kumari, S. e Khan, M.K., 2020a. "Porx: A reputation incentive scheme for blockchain consensus of iiot". *Future Generation Computer Systems*, Vol. 102, pp. 140–151.

Wang, Q., Zhu, X., Ni, Y., Gu, L. e Zhu, H., 2020b. "Blockchain for the iot and industrial iot: A review". *Internet of Things*, Vol. 10, p. 100081.

Wang, W., Xu, H., Alazab, M., Gadekallu, T.R., Han, Z. e Su, C., 2021. "Blockchain-based reliable and efficient certificateless signature for iiot devices". *IEEE Transactions on Industrial Informatics*.

Yu, K., Tan, L., Aloqaily, M., Yang, H. e Jararweh, Y., 2021. "Blockchain-enhanced data sharing with traceable and direct revocation in iiot". *IEEE Transactions on Industrial Informatics*, Vol. 17, pp. 7669–7678.

Yu, Y., Liu, S., Yeoh, P.L., Vucetic, B. e Li, Y., 2020. "Layerchain: a hierarchical edge-cloud blockchain for large-scale low-delay industrial internet of things applications". *IEEE Transactions on Industrial Informatics*, Vol. 17, No. 7, pp. 5077–5086.

Zhang, C. e Chen, Y., 2020. "A review of research relevant to the emerging industry trends: Industry 4.0, iot, blockchain, and business analytics". *Journal of Industrial Integration and Management*, Vol. 5, No. 01, pp. 165–180.

Zhang, P., Hong, Y., Kumar, N., Alazab, M., Alshehri, M.D. e Jiang, C., 2021. "Bc-edgefl: A defensive transmission model based on blockchain-assisted reinforced federated learning in iiot environment". *IEEE Transactions on Industrial Informatics*, Vol. 18, No. 5, pp. 3551–3561.

Zheng, T., Ardolino, M., Bacchetti, A. e Perona, M., 2021. "The applications of industry 4.0 technologies in manufacturing context: a systematic literature review". *International Journal of Production Research*, Vol. 59, No. 6, pp. 1922–1954.

Zuo, Y., 2021. "Making smart manufacturing smarter–a survey on blockchain technology in industry 4.0". *Enterprise Information Systems*, Vol. 15, No. 10, pp. 1323–1353.

8. RESPONSABILIDADE PELAS INFORMAÇÕES

O autor é o único responsável pelas informações incluídas neste trabalho.

BLOCKCHAIN IN INDUSTRY 4.0 - DEFINITION, APPLICABILITY AND DEVELOPMENT

Gabriel Arão [1]
Jones Yudi [2]
[1,2] Control and Automation Group, Universidade de Brasília
[1] gabriel.arao@aluno.unb.br, [2] jonesyudi@unb.br

Abstract:
Industry 4.0 is a term that refers to the adoption of various emerging technologies and new paradigms in various sectors of the industry such as Internet of Things, Artificial Intelligence, Cyber-Physical Systems, Virtualization, among others. This new industrial revolution ensures greater automation, productivity, quality, reliability, security, and efficiency compared to the traditional model, called Industry 3.0. In recent years, Blockchain has attracted attention for its successful use in cryptocurrencies, demonstrating its ability to create decentralized and secure record-keeping systems. Its security and efficiency characteristics, its conception based on already known technologies, and the relative simplicity of the idea ensure applicability in the most diverse contexts and have motivated the rapid evolution of the technology to adapt to the technical requirements of Industry 4.0. Currently, Blockchain is already considered one of the enabling technologies of the revolution that is Industry 4.0, providing greater transparency and traceability in industrial processes, a higher level of automation and ease in managing Internet of Things networks, as well as providing greater privacy and governance over data, facilitating the construction of collaborative and decentralized ecosystems, essential to ensure the rapid adaptability of the industry in a globally connected world with rapid and constant changes. In addition, the concept of tokenization existing in Blockchain aligns with the concept of cyber-physical systems of Industry 4.0, and can be naturally applied to improve the tracking of goods and the monitoring of the life cycle of products and machinery. This review article aims to present in detail what Blockchain is, the evolution of the technology since its conception, including the types of Blockchain, a representation of its general layered architecture, basic data structure, and the main commercial solutions available. Additionally, the state of the art in terms of Blockchain applications in Industry 4.0 is presented, which includes the management and security of Industrial Internet of Things devices, data storage and sharing, and applications in the industry such as supply chain and Smart Grid, with the main research and development trends also being discussed, highlighting the main problems and challenges currently open that must be overcome to ensure the evolution and popularization of the technology. Finally, the trend of technology adoption in Industry is presented, starting with the registration of transitions in supply chains, which is justified by the great benefits that can be obtained.

Palavras-chave: *Blockchain; Industry 4.0; IIoT; Cybersecurity*