UNIVERSIDADE FEDERAL DE OURO PRETO
INSTITUTO DE CIÊNCIAS EXATAS E BIOLÓGICAS
DEPARTAMENTO DE COMPUTAÇÃO

BIANCA MARCELINO SANTOS PEIXOTO
Orientador: Prof. Dr. Carlos Frederico Marcelo da Cunha Cavalcanti

# BLOCKCHAIN E NOVAS ENGINES PARA A INDÚSTRIA 4.0

Ouro Preto, MG
2025

UNIVERSIDADE FEDERAL DE OURO PRETO
INSTITUTO DE CIÊNCIAS EXATAS E BIOLÓGICAS
DEPARTAMENTO DE COMPUTAÇÃO

BIANCA MARCELINO SANTOS PEIXOTO

# BLOCKCHAIN E NOVAS ENGINES PARA A INDÚSTRIA 4.0

Monografia apresentada ao Curso de Ciência da Computação da Universidade Federal de Ouro Preto como parte dos requisitos necessários para a obtenção do grau de Bacharel em Ciência da Computação.

**Orientador:** Prof. Dr. Carlos Frederico Marcelo da Cunha Cavalcanti

Ouro Preto, MG
2025

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE OURO PRETO
REITORIA
INSTITUTO DE CIENCIAS EXATAS E BIOLOGICAS
DEPARTAMENTO DE COMPUTACAO

# FOLHA DE APROVAÇÃO

**Bianca Marcelino Santos Peixoto**

**Blockchain e novas *engines* para a indústria 4.0**

Monografia apresentada ao Curso de Ciência da Computação da Universidade Federal de Ouro Preto como requisito parcial para obtenção do título de Bacharel em Ciência da Computação

Aprovada em 16 de Abril de 2025.

Membros da banca

Doutor Carlos Frederico Marcelo da CUnha Cavalcanti (Orientador) - Universidade Federal de Ouro Preto
Doutor Ricardo Augusto Rabelo Oliveira (Examinador) - Universidade Federal de Ouro Preto
Mestre Vinicius Antônio de Oliveira Martins (Examinador) - Universidade Federal de Ouro Preto

Carlos Frederico Marcelo da Cunha Cavalcanti, Orientador do trabalho, aprovou a versão final e autorizou seu depósito na Biblioteca Digital de Trabalhos de Conclusão de Curso da UFOP em 28/04/2025.

Documento assinado eletronicamente por **Carlos Frederico Marcelo da Cunha Cavalcanti**, **CHEFE DO DEPARTAMENTO DE COMPUTAÇÃO**, em 22/04/2025, às 13:46, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.ufop.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0886267** e o código CRC **3C95A574**.



R. Diogo de Vasconcelos, 122, - Bairro Pilar Ouro Preto/MG, CEP 35402-163
Telefone: 3135591692 - www.ufop.br

# Agradecimentos

Gostaria de expressar minha sincera gratidão ao meu orientador, Prof. Dr. Carlos Frederico Marcelo da Cunha Cavalcanti, por toda a paciência, apoio e orientação ao longo desse processo. Suas sugestões, incentivo e confiança foram fundamentais para a realização deste trabalho. Agradeço, especialmente, por sempre estar disponível para tirar dúvidas e por me desafiar a buscar o melhor em cada etapa. Sou muito grata pela oportunidade de aprender com você.

Agradeço profundamente aos meus pais, que sempre estiveram ao meu lado durante toda a minha trajetória acadêmica e em todos os momentos importantes da minha vida. Obrigada por todo o amor, carinho e pelo apoio incondicional que recebo de vocês diariamente. Vocês são meu porto seguro e uma fonte constante de incentivo emocional e psicológico, fundamentais para que eu pudesse chegar até aqui. Tenho muita admiração pela dedicação, sabedoria e paciência de vocês. Sem o suporte constante, os conselhos valiosos e o exemplo de determinação que sempre me deram, certamente não teria conseguido alcançar essa conquista. Sou eternamente grata por tudo que fazem por mim e por todo o esforço que dedicam para me ver feliz e realizada.

Se a Indústria 4.0 é a máquina, a blockchain é o elo invisível que faz o futuro funcionar sem precisar confiar, apenas verificar. Autor anônimo, porém conhecido.

# Resumo

Este trabalho analisa a integração da tecnologia *blockchain* com a indústria 4.0, destacando benefícios como segurança, transparência e automação em processos industriais. O objetivo principal foi analisar como o *blockchain* pode ser integrado aos processos industriais para aprimorar a segurança, transparência e eficiência operacional do setor. Para alcançar esse objetivo, foram identificadas as tecnologias e princípios fundamentais da indústria 4.0 relacionados à *blockchain*, avaliando-se as vantagens e obstáculos da sua implementação no ambiente industrial. Experimentalmente, foram desenvolvidas e analisadas redes privadas baseadas em Ethereum e Cosmos, integradas com um banco de dados PostgreSQL, e realizados testes comparativos que avaliaram aspectos de desempenho como latência, tempo de processamento de blocos e escalabilidade. Os resultados destacaram que a plataforma Cosmos apresentou melhor desempenho operacional, maior estabilidade e eficiência, reforçando o potencial dessa abordagem híbrida para atender às necessidades específicas da indústria 4.0.

**Palavras-chave**: Blockchain. Indústria 4.0. Ethereum. Cosmos. Redes privadas. Automação industrial.

# Abstract

This study analyzes the integration of blockchain technology with industry 4.0, highlighting benefits such as security, transparency, and automation in industrial processes. The main objective was to analyze how blockchain can be integrated into industrial processes to enhance security, transparency, and operational efficiency of the sector. To achieve this goal, the fundamental technologies and principles of industry 4.0 related to blockchain were identified, evaluating the advantages and obstacles of its implementation in industrial environments. Experimentally, private networks based on Ethereum and Cosmos integrated with a PostgreSQL database were developed and analyzed, with comparative tests evaluating performance aspects such as latency, block processing time, and scalability. The results highlighted that the Cosmos platform demonstrated superior operational performance, greater stability, and efficiency, reinforcing the potential of this hybrid approach to meet the specific needs of industry 4.0.

**Keywords**: Blockchain. Industry 4.0. Ethereum. Cosmos. Private networks. Industrial automation.

# Lista de Ilustrações


Figura 2.1 – Evolução das revoluções industriais até a Indústria 4.0. Fonte: Adaptado de Wolf Automation (Wolf Automation, 2024). . . . . 5
Figura 2.2 – Interconexão de tecnologias emergentes na indústria 4.0. Fonte: Adaptado de ResearchGate (MISHRA; MOHANTA; MAHANTY, 2022). . . . . 9
Figura 2.3 – Processo de funcionamento de uma *blockchain*, desde a solicitação de uma transação até a validação e sua inclusão no bloco final. Fonte: Adaptado de GeeksforGeeks (GeeksforGeeks, 2024b). . . . . 11
Figura 2.4 – Interconexão de tecnologias emergentes na indústria 4.0. Fonte: Adaptado de IoTHub (IoTHub, 2024). . . . . 12
Figura 2.5 – Integração da *blockchain* e IoT na manufatura inteligente com monitoramento em tempo real. Fonte: Adaptado de Altoros (Altoros, 2024). . . . . 13
Figura 2.6 – Estrutura dos blocos em uma *blockchain*. Fonte: Adaptado de GeeksforGeeks (GeeksforGeeks, 2024a). . . . . 18
Figura 2.7 – Benefícios da *blockchain* na cadeia de suprimentos. Fonte: Adaptado de AWS (Amazon Web Services, 2024). . . . . 23
Figura 2.8 – Etapas de funcionamento de um contrato inteligente na *blockchain*. . . . . 24
Figura 2.9 – Desafios e limitações da adoção da *blockchain* na cadeia de suprimentos. Fonte: Adaptado de AWS (Amazon Web Services, 2024). . . . . 26
Figura 3.1 – Interconexão entre máquinas executando a Ethereum Virtual Machine (EVM). Fonte: Adaptado de Núcleo do Conhecimento (Nucleo do Conhecimento, 2024). 31
Figura 3.2 – Fluxo de compilação do código Solidity até a implantação no Ethereum Virtual Machine. Fonte: Adaptado de Metlabs (Metlabs, 2024). . . . . 33
Figura 3.3 – Comparação entre *proof of work* e *proof of stake*. Fonte: Adaptado de SketchBubble (SketchBubble, 2024). . . . . 34
Figura 3.4 – Comparação entre arquitetura cliente-servidor e arquitetura P2P. Fonte: Adaptado de Medium (Nilay Güler, 2024). . . . . 38
Figura 3.5 – Funcionamento do Mempool e priorização de transações no Ethereum. Fonte: Adaptado de Hub do Investidor (Hub do Investidor, 2024). . . . . 43
Figura 3.6 – Comparação entre PoW e PoS no Ethereum. Fonte: Adaptado de Luo Zhu (Luo Zhu, 2024). . . . . 44
Figura 3.7 – Arquitetura distribuída em múltiplos hubs e zonas no Cosmos Network. Fonte: Adaptado de Preethi Kasireddy (KASIREDDY, 2020). . . . . 49
Figura 3.8 – Comunicação entre zonas via IBC. Fonte: Adaptado de Preethi Kasireddy (KASIREDDY, 2020). . . . . 51
Figura 3.9 – Estrutura funcional de um hub no Cosmos. Fonte: Adaptado de Preethi Kasireddy (KASIREDDY, 2020). . . . . 54

Figura 4.1 – Exemplo de configuração do bloco gênesis no arquivo genesis.json. . . . . 59
Figura 4.2 – Defininfo variáveis de ambiente. . . . . 60
Figura 4.3 – Dockerfile para inicializar a rede Ethereum usando Geth. . . . . 61
Figura 4.4 – Comando para gerar a chave criptográfica do *bootnode*. . . . . 62
Figura 4.5 – Formato do identificador enode com IP e porta. . . . . 62
Figura 4.6 – Comando para gerar o enode a partir da chave do nó. . . . . 62
Figura 4.7 – Comando para construir e iniciar a rede usando Docker Compose. . . . . 67
Figura 4.8 – Comando para enviar uma transação Ethereum. . . . . 68
Figura 4.9 – Comando para recuperar uma transação pelo *hash*. . . . . 68
Figura 4.10–Comando utilizado para a criação da estrutura inicial do projeto de *blockchain*. 69
Figura 4.11–Comando usado para criar a estrutura inicial do seu projeto de *blockchain*. . 70
Figura 4.12–Configuração presente no arquivo config.yml . . . . . 70
Figura 4.13–Configuração presente no arquivo config.yml . . . . . 70
Figura 4.14–Configuração presente no arquivo config.yml . . . . . 71
Figura 4.15–Comando de inicialização da *blockchain*. . . . . 71
Figura 4.16–Comando de realização de transações dentro da *blockchain*. . . . . 71
Figura 5.1 – Distribuição comparativa dos tempos médios de extração de blocos . . . . . 73
Figura 5.2 – Variação do throughput transacional ao longo de 24 horas . . . . . 75
Figura 5.3 – Representação gráfica do tempo médio de processamento do bloco . . . . . 77
Figura 5.4 – Representação gráfica da latência de rede . . . . . 79
Figura 5.5 – Representação gráfica do throughput transacional . . . . . 80

# Lista de Tabelas

Tabela 5.1 – Análise temporal da extração de blocos por minerador . . . . . 72
Tabela 5.2 – Análise qualitativa das características operacionais dos mineradores . . . . . 74
Tabela 5.3 – Correlação entre latência de rede e eficiência operacional por minerador . . 74
Tabela 5.4 – Análise estatística do throughput transacional por minerador . . . . . 76
Tabela 5.5 – Distribuição do tempo médio de processamento de blocos por validador na rede Cosmos . . . . . 77
Tabela 5.6 – Distribuição da latência média por validador na rede Cosmos . . . . . 78
Tabela 5.7 – Distribuição do throughput transacional por validador na rede cosmos . . . 80
Tabela 5.8 – Distribuição do número médio de transações por bloco na rede Cosmos . . . 81
Tabela 5.9 – Análise comparativa do tempo de processamento entre Ethereum e Cosmos 82
Tabela 5.10–Análise comparativa da latência de rede entre Ethereum e Cosmos . . . . . 83
Tabela 5.11–Análise comparativa do throughput transacional entre ethereum e cosmos . . 84
Tabela 5.12–Síntese comparativa das características fundamentais de Ethereum e Cosmos 86

# Lista de Abreviaturas e Siglas

| | |
|---|---|
| SHA-256 | Secure Hash Algorithm 256 |
| Keccak | Secure Hash Algorithm 3 |
| BLS | Boneh-Lynn-Shacham |
| ECDSA | Elliptic Curve Digital Signature Algorithm |
| RLP | Recursive Length Prefix |
| SSZ | Simple Serialization |
| VRF | Verifiable Random Function |
| VDF | Verifiable Delay Function |
| PoW | Proof of Work |
| PoS | Proof of Stake |
| DPoS | Delegated Proof of Stake |
| P2P | Peer-to-Peer |
| DoS | Denial of Service |
| IP | Internet Protocol |
| IoT | Internet of Things |
| LibP2P | Library Peer-to-Peer |
| DevP2P | Developer Peer-to-Peer |
| Discv5 | Discovery Version 5 |
| Discv4 | Discovery Version 4 |
| BFT | Byzantine Fault Tolerance |
| EVM | Ethereum Virtual Machine |
| DNS | Domain Name System |
| dApp | Decentralized Applications |

# Sumário


**1 Introdução . . . . . 1**
1.1 Justificativa . . . . . 1
1.2 Objetivos . . . . . 2
1.3 Organização do Trabalho . . . . . 2
**2 Revisão Bibliográfica . . . . . 3**
2.1 Introdução . . . . . 3
2.2 Trabalhos Relacionados . . . . . 3
2.3 Fundamentação Teórica . . . . . 4
2.3.1 Introdução . . . . . 4
2.3.2 Indústria 4.0 . . . . . 5
2.3.3 Princípios Fundamentais da Indústria 4.0 . . . . . 6
2.3.4 Tecnologias-chave da indústria 4.0 . . . . . 7
2.3.5 Tecnologia Blockchain . . . . . 9
2.4 Impactos da Blockchain na Indústria . . . . . 11
2.4.1 Cadeias de Suprimentos e Logística . . . . . 11
2.4.2 Manufatura Inteligente . . . . . 12
2.4.3 Comércio de Energia . . . . . 14
2.4.4 Indústria Farmacêutica e Saúde . . . . . 14
2.4.5 Seguros . . . . . 15
2.4.6 Setor Público e Governança . . . . . 16
2.4.7 Componentes Chave da Blockchain: . . . . . 16
2.5 Algoritmos de Consenso . . . . . 19
2.5.1 Proof of Work (PoW) . . . . . 19
2.5.2 Proof of Stake (PoS) . . . . . 20
2.5.3 Delegated Proof of Stake (DPoS) . . . . . 21
2.6 Aplicações de blockchain na indústria 4.0 . . . . . 22
2.6.0.1 Rastreabilidade de cadeia de suprimentos . . . . . 22
2.6.0.2 Smart contracts (contratos inteligentes) . . . . . 23
2.6.0.3 Segurança de dados e privacidade . . . . . 24
2.6.0.4 Manutenção preditiva . . . . . 25
2.6.0.5 Autenticação e combate à falsificação . . . . . 25
2.6.1 Desafios e limitações . . . . . 25
2.6.1.1 Escalabilidade . . . . . 26
2.6.1.2 Custo e a complexidade . . . . . 26
2.6.1.3 Interoperabilidade . . . . . 27
2.6.1.4 Impacto Ambiental . . . . . 27

2.6.1.5 Tempo de Validação e Latência . . . 27
2.6.1.6 Segurança em Redes Híbridas . . . 28
2.6.1.7 Governança Descentralizada . . . 28
2.6.1.8 Privacidade dos Dados . . . 28
2.6.1.9 Barreiras Culturais e Resistência à Mudança . . . 29
2.6.2 Conclusão . . . 29
**3 Plataformas Blockchain . . . 30**
3.1 Introdução ao Ethereum . . . 30
3.1.1 Conceito e Contextualização . . . 30
3.2 Arquitetura do Ethereum . . . 31
3.2.1 Camada de Execução . . . 31
3.2.2 Camada de Consenso . . . 33
3.2.3 Camada de Rede . . . 34
3.2.4 Camada de Aplicação . . . 35
3.3 Geth (Go-Ethereum) . . . 35
3.3.1 O que é o Geth? . . . 35
3.3.2 Clientes Ethereum . . . 36
3.3.2.1 Clientes de Execução . . . 36
3.3.2.2 Clientes de Consenso . . . 37
3.3.3 Beacon Client . . . 37
3.4 Aspectos Técnicos . . . 38
3.4.1 Networking . . . 38
3.4.1.1 Estrutura de Rede P2P . . . 38
3.4.1.2 Comunicação através de Protocolos . . . 39
3.4.2 Peer Discovery & Management . . . 39
3.4.2.1 Resistência a Ataques Sybil na Rede Ethereum . . . 39
3.4.2.2 Prevenção de DoS . . . 40
3.4.2.3 Pontuação de Nós na Rede Ethereum . . . 40
3.4.2.4 Propagação de Dados na Rede Ethereum . . . 40
3.4.2.5 Rastreamento da Árvore de Blocos . . . 41
3.4.2.6 Reorganizações de Blockchain e Resolução de Forks . . . 41
3.4.2.7 Mempool de Transações no Ethereum . . . 42
3.4.2.8 Sincronização . . . 43
3.5 Comparação das Tecnologias do Ethereum . . . 44
3.5.1 Introdução . . . 44
3.5.2 LibP2P . . . 45
3.5.3 DevP2P . . . 45
3.5.4 BLS vs ECDSA . . . 47
3.6 Introdução ao Cosmos Network . . . 48

3.6.1 Arquitetura do Cosmos . . . 49
3.6.1.1 Cosmos SDK . . . 49
3.6.1.2 Tendermint Core . . . 50
3.6.1.3 Inter-Blockchain Communication (IBC) . . . 50
3.6.2 Ferramenta Principal . . . 51
3.6.2.1 Starport . . . 51
3.6.3 Aspectos Técnicos . . . 53
3.6.3.1 Estruturas de Rede no Cosmos . . . 53
3.6.3.2 Mecanismos de Consenso (Tendermint) . . . 54
3.6.3.3 Comunicação entre Blockchains . . . 55
3.6.4 Comparação com Ethereum . . . 55
3.6.4.1 Arquitetura e Modularidade . . . 55
3.6.4.2 Interoperabilidade . . . 56
3.6.4.3 Escalabilidade e Eficiência . . . 56
3.6.4.4 Mecanismo de Consenso . . . 56
3.6.4.5 Aplicações e Usabilidade . . . 57
3.6.4.6 Conclusão Comparativa . . . 57
**4 Experimentação Prática . . . 58**
4.1 Introdução . . . 58
4.2 Configuração da Rede Privada Ethereum . . . 58
4.2.1 Bloco Gênesis e Arquivo de Configuração genesis.json . . . 58
4.2.2 Arquivo .env e Configuração de Variáveis . . . 60
4.2.3 Criação do Dockerfile e Automação da Inicialização . . . 60
4.2.4 Configuração do Bootnode e Enode . . . 61
4.2.5 Arquivo docker-compose.yml e Conectividade da Rede . . . 62
4.3 Execução da Rede e Mineração . . . 67
4.3.1 Validação de Blocos e Sincronização de Nós . . . 67
4.3.2 Realização de Transações . . . 68
4.3.3 Transações Automáticas . . . 68
4.4 Configuração da Rede Privada Cosmos . . . 68
4.4.1 Configuração do Ambiente . . . 69
4.4.2 Inicialização do Projeto . . . 69
4.4.3 Configuração da Rede Blockchain . . . 70
4.5 Execução da Rede . . . 71
4.5.1 Realização de Transações . . . 71
**5 Resultados . . . 72**
5.1 Análise dos Resultados . . . 72
5.2 Resultados na Rede Ethereum . . . 72
5.2.1 Análise Paramétrica do Desempenho dos Mineradores . . . 72

5.2.2 Análise da Relação entre Latência e Eficiência Operacional . . . . . 74
5.2.3 Análise do Throughput Transacional . . . . . 75
5.2.4 Discussão das Implicações Tecnológicas . . . . . 76
5.3 Resultados na Rede Cosmos . . . . . 77
5.3.1 Análise do Tempo de Processamento de Blocos . . . . . 77
5.3.2 Análise da Latência de Rede . . . . . 78
5.3.3 Análise do Throughput Transacional . . . . . 79
5.3.4 Análise da Capacidade de Processamento por Bloco . . . . . 81
5.3.5 Discussão das Implicações Tecnológicas . . . . . 81
5.4 Análise Comparativa entre Ethereum e Cosmos . . . . . 82
5.4.1 Análise Comparativa do Tempo de Processamento . . . . . 82
5.4.2 Análise Comparativa da Latência de Rede . . . . . 83
5.4.3 Análise Comparativa do Throughput Transacional . . . . . 84
5.4.4 Análise da Variabilidade do Desempenho . . . . . 84
5.4.5 Análise das Implicações para Aplicações Práticas . . . . . 85
5.4.6 Síntese Comparativa . . . . . 86
5.5 Conclusões e Perspectivas . . . . . 87
**6 Considerações Finais . . . . . 88**
6.1 Conclusão . . . . . 88
6.2 Reflexões sobre Blockchain e Indústria 4.0 . . . . . 88
6.3 Contribuições do Trabalho . . . . . 89

**Referências . . . . . 90**

# 1 Introdução

A Indústria 4.0 tem remodelado os sistemas produtivos, transformando-os em ambientes onde tecnologias emergentes são integradas para otimizar processos, aumentar a produtividade e viabilizar novos modelos de negócio. Nesse cenário, destaca-se a tecnologia *blockchain*, que proporciona segurança, transparência e rastreabilidade das informações (BODKHE et al., 2020). Por operar como um sistema distribuído e descentralizado, a *blockchain* é reconhecida como um dos pilares fundamentais da Indústria 4.0.

Esse novo paradigma industrial é caracterizado pela convergência entre os mundos físico e digital, impulsionado por avanços significativos em inteligência artificial, internet das coisas, automação e processamento de informações (TYAGI et al., 2023). No entanto, tal evolução tecnológica impõe desafios complexos, especialmente em relação à interoperabilidade entre sistemas heterogêneos e à gestão eficiente de grandes volumes de dados e transações. Nesse contexto, a tecnologia *blockchain*, por ser um sistema de registro distribuído que viabiliza transações seguras e diretas sem intermediários, apresenta-se como uma solução promissora para enfrentar esses desafios.

Embora originalmente associada ao setor financeiro e às criptomoedas, a *blockchain* tem expandido seu uso para diversas áreas como manufatura, logística e cadeias de suprimentos. No âmbito da Indústria 4.0, promete revolucionar o controle dos processos produtivos ao assegurar autenticidade, eficiência operacional e confiança entre as partes envolvidas, especialmente por meio de contratos inteligentes (*smart contracts*) e redes descentralizadas (MOURTZIS; ANGELOPOULOS; PANOPOULOS, 2023).

Neste trabalho, será investigada a integração da tecnologia *blockchain* com os conceitos e processos da Indústria 4.0, com ênfase na implementação prática de redes privadas baseadas em Ethereum e Cosmos. Serão analisadas as oportunidades proporcionadas por essa integração tecnológica e sua potencial contribuição para enfrentar os principais desafios da indústria contemporânea.

## 1.1 Justificativa

Toda a argumentação sobre o tópico desta pesquisa foi agregada pelo crescente importância do *blockchain* na indústria. Como as organizações são parte da realidade em que operam e é preciso inovar e modernizar seus sistemas antigos constantemente, o conceito de indústria 4.0 é aplicado no que se refere as novas tecnologias se comunicando diretamente por meio de dados. Atualmente, segurança, armazenagem eficiente e transferência rápida e precisa de informações são vitais para as empresas e o *blockchain* supera em muito as tecnologias tradicionais existentes

neste sentido.

Ademais, a integração do *blockchain* nos processos de produção na indústria 4.0 pode resultar em maior competitividade. Este estudo visa apoiar de forma prática na aplicação do *blockchain* na indústria 4.0, discutindo as oportunidades e desafios que ele apresenta.

## 1.2 Objetivos

O objetivo principal deste trabalho é analisar a integração da tecnologia *blockchain* aos processos da indústria 4.0, visando aprimorar a segurança, transparência e eficiência operacional do setor. Para alcançar esse objetivo geral, os seguintes objetivos específicos foram estabelecidos:

- Identificar as tecnologias e os princípios fundamentais da indústria 4.0 relacionados à *blockchain*;
- Avaliar as vantagens e obstáculos na implementação da tecnologia *blockchain* no ambiente industrial;
- Analisar e validar aplicações práticas da *blockchain* por meio de experimentos com redes privadas Ethereum e Cosmos, comparando aspectos de desempenho como latência, tempo de processamento e escalabilidade.

## 1.3 Organização do Trabalho

Este estudo está organizado em cinco seções:

- Capítulo 1: Apresentação da introdução, justificativa e metas do estudo.
- Capítulo 2: Análise bibliográfica sobre indústria 4.0 e *blockchain*, abrangendo pesquisas correlatas e a base teórica.
- Capítulo 3: Plataformas Blockchain: Ethereum e Cosmos.
- Capítulo 4: Técnica utilizada para a execução da pesquisa.
- Capítulo 5: Exposição e debate dos achados, fundamentados nos estudos de caso e análises conduzidas.
- Capítulo 6: Encerramento do estudo, apresentando um resumo das descobertas e recomendações para estudos futuros.

# 2 Revisão Bibliográfica

## 2.1 Introdução

O uso do *blockchain* na Indústria 4.0 é um tópico emergente com interesse crescente entre pesquisadores e profissionais da área. O potencial dessa tecnologia em transformar diversos processos industriais tem motivado o desenvolvimento de estudos significativos, destacados neste capítulo. Desta forma, esta seção explora pesquisas recentes sobre como a tecnologia *blockchain* pode beneficiar principalmente a automação, a segurança e a eficiência industrial. As principais contribuições revisadas incluem a integração do *blockchain* com sistemas de gêmeos digitais, inovações em mecanismos de consenso e avanços na segurança cibernética. Portanto, o propósito deste capítulo é analisar essas abordagens principais e identificar áreas que ainda demandam maior investigação, oferecendo assim uma visão abrangente das tendências e lacunas existentes no campo.

## 2.2 Trabalhos Relacionados

A aplicação de tecnologias de *blockchain* na indústria 4.0 tem sido o ponto focal de um bom número de estudos e pesquisas práticas nos últimos anos. Esta parte fornece uma revisão de alguns desses trabalhos relacionados, identificando suas contribuições importantes e as lacunas ou oportunidades para novos estudos. Algumas dessas pesquisas têm sido sobre como o *blockchain* pode se encaixar nos processos da indústria 4.0.

Por exemplo, (GARROCHO, 2022) explica várias arquiteturas para a integração de sistemas de automação baseados em *blockchain* no processo industrial. (TEISSERENC; SEPASGOZAR, 2021) propôs um modelo conceitual de integração do *blockchain* em gêmeos digitais das indústrias *BECOM* 4.0—significando *Building, Engineering, Construction, Operations, and Mining*. Para incentivar maior confiabilidade, segurança, eficácia e sustentabilidade ao longo dos projetos, o modelo incorpora os seguintes aspectos: identifica desafios principais e faz uma abordagem *PESTELS* (*Political, Economic, Social, Technological, Legal, and Environment*) para o ciclo de vida da Cadeia Descentralizada de Gêmeos Digitais—*DDTC* como uma estrutura tecnológica. É um modelo que integra *blockchain*, a Internet das Coisas, *BIM* (*Building Information Modeling*) e gêmeos digitais para abordar a governança de redes, escalabilidade, interoperabilidade, eficiência energética e necessidades computacionais.

(BODKHE et al., 2020) acrescentou que a solução oferecida pelo *blockchain* para aplicações da indústria 4.0—mais especificamente agricultura inteligente, saúde e logística—estava alinhada com a redução de preocupações com segurança e privacidade instigadas pela exploração

da *Internet* na transferência de dados. Ele faz uma comparação entre soluções centralizadas e *blockchain*, concentrando-se em certas áreas nas quais o *blockchain* pode agregar valor. Em questões de escalabilidade, robustez, armazenamento de dados, latência de rede, auditabilidade, imutabilidade e rastreabilidade, o *blockchain* pode agregar valor.

(MOURTZIS; ANGELOPOULOS; PANOPOULOS, 2023) destaca que o aumento da eficiência na fabricação inteligente e a cibersegurança, impulsionados pela indústria 5.0 e pelo metaverso industrial, estão diretamente ligados à proteção de dados e à organização da comunicação por meio de bancos de dados distribuídos e descentralizados na indústria 4.0.

(HOSSAIN; BADSHA; SHEN, 2020) também discutiu a implementação da tecnologia *blockchain* em redes inteligentes e indústria 4.0. Nos sistemas *SCADA* (*Supervisory Control and Data Acquisition*), é necessário ter descentralização, operações em quase tempo real, segurança e privacidade. Além disso, o autor propôs que a Prova de Contagem Aleatória em *Hashes* (*PoRCH*) pode ser um novo mecanismo de consenso na introdução do *blockchain* no *SCADA*.

(EL-DIN et al., 2024) propôs uma estrutura para a integração de Gêmeos Digitais com *blockchain* para melhorar o desempenho dos Contratos de Desempenho Energético (*EPCs*) em um ambiente onde há desafios relacionados ao compartilhamento, armazenamento e segurança de dados.

(AHAKONYE; NWAKANMA; KIM, 2024) propôs sua integração com Sistemas de Detecção de Intrusões (*IDS*) em redes IoT como uma medida para melhorar a segurança. Khan propôs um modelo híbrido de previsão que abrange Redes Neurais Recorrentes, Memória de Longo Prazo (*LSTM*) e Unidades Recorrentes com Portas (*GRU*) otimizadas por Algoritmos Genéticos (*GA*). O objetivo é treinar profissionais da cadeia de suprimentos para usar essas tecnologias avançadas e capacitar a indústria na formulação de políticas com base nas previsões avançadas de aprendizado profundo.

## 2.3 Fundamentação Teórica

### 2.3.1 Introdução

A indústria 4.0 posiciona-se de maneira inédita no que se refere à forma, à mudança e ao desenvolvimento do atual modo de produção industrial. Ao contrário das revoluções anteriormente observadas, centradas, principalmente, em mecanização e automação, por meio da combinação de tecnologias digitais avançadas, busca-se obter um ambiente de produção mais inteligente, conectado e autônomo. Assim sendo, a indústria 4.0 incide na interseção do físico com o digital, sendo impulsionada por Inteligência Artificial, Internet das Coisas, *blockchain* e *Big Data*.

A convergência tecnológica possibilita que fábricas e cadeias de suprimento respondam de forma mais eficiente, flexível e autônoma às mudanças do mercado e às demandas personalizadas dos clientes. Com isso, a nova era da indústria 4.0 abre um novo espaço para modelos de negócios

e processos de fabricação conectados em tempo real, além do uso de dados inteligentes. Um dos aspectos mais disruptivos é a importância que o *blockchain* assume, garantindo a segurança, rastreabilidade e integridade dos dados num ambiente industrial cada vez mais descentralizado e automatizado.

Com isso, inovação, eficiência e flexibilidade são empregadas na forma como a logística e as relações entre produtores e consumidores são radicalmente remodeladas. Altera-se profundamente a natureza da produção e organização empresarial, criando oportunidades para valores de eficiência, produção e concepção que nem sequer existiam anos atrás.

A Figura 2.1 a seguir mostra como as revoluções industriais evoluíram, destacando os principais marcos tecnológicos de cada era. Desde a mecanização na indústria 1.0, passando pela eletrificação e automação, até a indústria 4.0, percebe-se um processo evolutivo no qual a integração de sistemas ciberfísicos e tecnologias emergentes, como *blockchain* e Internet das Coisas (IoT), desempenha um papel fundamental.

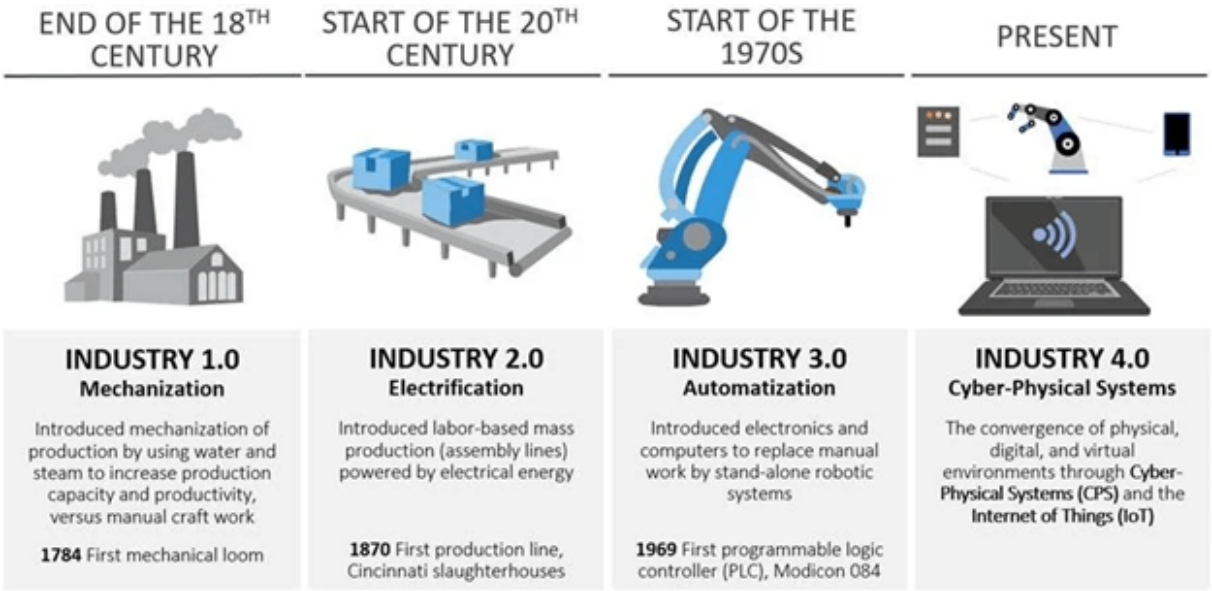


Figura 2.1 – Evolução das revoluções industriais até a Indústria 4.0. Fonte: Adaptado de Wolf Automation (Wolf Automation, 2024).

### 2.3.2 Indústria 4.0

A indústria 4.0 está introduzindo uma nova fase de integração tecnológica na produção. As estruturas de comércio se convertem em sistemas independentes, onde equipamentos, utensílios e programas interagem de forma constante. A combinação de tecnologias essenciais como a Internet das Coisas, Inteligência Artificial, *Big Data*, computação em nuvem e *blockchain* é responsável por isso. Estas tecnologias, quando combinadas, criam um ecossistema de produção inteligente. Aqui, todas as decisões automatizadas são fundamentadas em dados coletados e os processos são constantemente aprimorados para se tornarem mais eficazes ou ecológicos.

Ainda, uma das maiores conquistas é a geração de gêmeos digitais do ciclo de vida de ativos, produtos, processos e fábricas completas. Eles podem ser usados para supervisionar e gerenciar operações remotamente. E quando itens são produzidos com customização em massa, configurados para atender às necessidades específicas e às demandas dos clientes, isso pode ser feito sem comprometer a eficácia. Nesse sentido, é possível dizer que todas as transações e interações têm o *blockchain* no cerne, uma vez que é fundamental para garantir que todas as transações e ações sejam protegidas, auditáveis e imutáveis. Isso tudo só é possível porque vivemos em um mundo digital que agora é também distribuído.

### 2.3.3 Princípios Fundamentais da Indústria 4.0

Os princípios básicos que orientam essa nova fase tecnológica são baseados na aplicação de inovações para converter indústrias em fábricas inteligentes e interconectadas. A seguir estão os quatro pilares que sustentam esse sistema:

- Interoperabilidade: Significa que qualquer sistema, máquina ou dispositivo consegue se conectar com IoT. Isto permite fluidez em dados de alta precisão até mesmo sob serviços secundários. Essa troca de dados ultraeficiente estabelece que a operação normal de fábricas seja precisa e sincronizada. Com uma cadeia de suprimentos integrada, que envolve tanto fornecedores globais quanto locais, essa integração em nível global torna-se fundamental.
- Transparência da informação: Os sensores instalados nos equipamentos e sistemas podem coletar dados ao vivo. Isso dá a visão corrente da situação das diferentes fases de fabricação. Com tais informações em suas mãos, gestores podem tomar decisões rápidas e bem informadas. Assim, podem impedir falhas antes de acontecerem sem arruinar a linha de produção. A transparência desse tipo é fortalecida pelo *blockchain*, por meio da segurança, imutabilidade e confiabilidade adicionais que os dados reunidos terão.
- Suporte técnico: A tecnologia oferece dois tipos de suporte, assistência ao operador humano na tomada de decisões, e assistência na execução de tarefas perigosas, repetitivas ou exaustivas. E isso é realizado por meio de sistemas automáticos, como robôs com inteligência artificial ou robóticas colaborativas (*Cobots*), que trabalham em conjunto com humanos para aumentar a segurança e produtividade, assim, liberando a mão de obra para tarefas de mais alto valor.
- Descentralização: Em vez de controle centralizado, os sistemas ciberfísicos e redes inteligentes coordenam e otimizam os processos de produção no nível local com capacidade de resposta imediata às mudanças no mercado. Esse sistema também é resiliente porque as decisões descentralizadas permitem que as operações continuem eficazes, mesmo em casos de falhas específicas. Além disso, o *blockchain* garante que essas decisões descentralizadas sejam verificadas e seguras em um ambiente de confiança, sem a necessidade de uma autoridade central.

### 2.3.4 Tecnologias-chave da indústria 4.0

A indústria 4.0 é a quarta revolução industrial. Suas características principais são a ocorrência de tecnologias digitais de ponta que permitem que toda a cadeia produtiva seja incluída no universo digital. É revolucionária para a indústria de todos os ângulos, desde como as indústrias são estruturadas, como tomam decisões, até como estão associadas ao universo produtivo. No entanto, diferentemente das três revoluções anteriores, que trouxeram inovações puramente mecânica, eletrônica e de automação, a indústria 4.0 é baseada em sistemas físicos e digitais, conectados através de redes de tecnologia digital, que oferece maiores possibilidades de inserção de flexibilidade, automação e personalização em massa. Não é apenas uma revolução técnica; é uma mudança estrutural no sistema de varejo de cadeias de suprimento, como os conhecemos hoje. No centro desta revolução industrial, há algumas tecnologias-chave que, quando combinadas, são muito mais produtivas, efetivas e sustentáveis. Estas tecnologias estão mais inteligentes, pois podem capturar, analisar e fazer a diferença com dados reais, são autônomas, com menos risco de cometer erros, e proporcionam uma melhor forma de otimizar recursos. Essa combinação representa, ao mesmo tempo, uma nova oportunidade de negócio e uma economia proativa e robusta que se integra ao domínio global. As tecnologias-chave que impulsionam a nova era industrial são:

A internet das coisas (*Internet of Things* - IoT) é uma ampla rede de objetos, máquinas e veículos que estão equipados com sensores para coleta de dados. Eles estão integrados à internet para comunicação e troca de dados em tempo real. Como parte da indústria 4.0, a *Internet of Things* tornará possível monitorar as coisas de perto e fazer manutenção preditiva e automação. A IoT utilizará dados de sensores ao longo de toda a linha de produção, fornecendo as informações necessárias para aumentar a eficiência das operações corporativas e orientar a tomada de decisões em tempo real (LEE; LEE, 2015).

A inteligência artificial (*Artificial Intelligence* - AI) desempenha importante trabalho no processamento de tais dados e no gerenciamento dos volumes produzidos pela IoT. A AI identifica padrões, antecipa a ocorrência das falhas, a falha em si e a resolução da falha antes de sua ocorrência, otimizando os processos de produção. Além disso, graças à AI, é possível otimizar a revolução da personalização em massa, pois se os processos de produção puderem ser modificados com base nas preferências e na demanda dos consumidores, não haverá perda de eficiência. Por exemplo, na Amazon, mudanças simples na quantidade de um produto baseadas em predições afetam a forma como os produtos são armazenados, embalados e enviados (GARCÍA et al., 2019).

Computação em nuvem (*Cloud Computing*) é uma infraestrutura versátil e expansível que proporciona acesso ininterrupto a sistemas e dados de diferentes setores ao redor do mundo, desde que a região de destino tenha capacidade de processamento de dados. O conceito de computação em nuvem é baseado no acesso sob demanda, permitindo que os recursos de computação estejam disponíveis 24 horas por dia, sem a necessidade de investir na compra de hardware próprio. Na

indústria 4.0, garante a interconexão complexa de sistemas inteligentes, prestando suporte e cooperação entre diferentes partes e unidades de uma cadeia de suprimentos em tempo real, além de requerer a continuidade do processamento computacional e analítico (HASHEM et al., 2014).

A manufatura aditiva (*Additive Manufacturing*) ou impressão 3D altera drasticamente a produção industrial. Atualmente, a impressão 3D permite a produção com precisão de peças complexas e com menores índices de desperdício de material. Nesse processo, o *blockchain* surge mais uma vez, ao tornar a propriedade dos desenhos digitais (arquivos CAD) de peças digitais evidente, além de garantir a rastreabilidade dos materiais e peças. O *blockchain* torna a informação sobre todas as etapas da produção do produto final aditiva imutável, sendo transparente e segura. Para tornar a propriedade e transferência da peça autônoma, é utilizada a tecnologia de contratos inteligentes do *blockchain*, que acionam pagamentos após a verificação dos parâmetros de produção, para serem liberados (GEBHARDT, 2011).

A realidade aumentada, mais conhecida como *Augmented Reality* (AR), já está sendo usada para tarefas de operação e manutenção industrial. Ao sobrepor informações digitais ao mundo físico, a AR pode fornecer ao operador informações mais claras sobre o processo ou contexto. Devido a isso, a precisão e segurança da operação são definitivamente melhoradas. Outra ferramenta que pode ajudar a habilitar essa opção em amplo uso é o *blockchain*. Fundamentalmente, o *blockchain* pode garantir a autenticidade de todas as informações utilizadas pela AR. Isso aumentará ainda mais a eficácia da AR, garantindo que as instruções ou informações fornecidas possam ser confortavelmente imutáveis. Por fim, o *blockchain* também pode ser usado para rastrear todas as operações guiadas pela AR. Ele irá ajudar a manter um registro de todas as ações que um operador ou programador faz. Isso permite uma trilha auditável das operações (MEKNI; LEMIEUX, 2014).

O *blockchain* proporciona uma camada extra de transparência, segurança e rastreabilidade. Com o registro imutável de transações, e os contratos inteligentes que regulamentam automática e transparentemente um conjunto de regras e regulamentos, o *blockchain* na indústria 4.0 aumenta a eficiência e a confiança entre os acionistas em uma cadeia de produção distribuída (BODKHE et al., 2020).

A combinação de IoT, inteligência artificial, computação em nuvem, manufatura aditiva e realidade aumentada, com *blockchain* fornecerá oportunidade de revolucionar processos. A redução de despesas, meios mais versáteis de produção e modelos de negócios novos unidos à nova geração de organizações, são cruciais para as organizações se manterem competitivas diante do cenário global de maior dinamicidade de mercado e avanço tecnológico.

A automatização e digitalização de processos da indústria 4.0 por meio das tecnologias emergentes, bem como sua interconexão e interação ao longo de uma cadeia produtiva, são apresentadas na Figura 2.2.

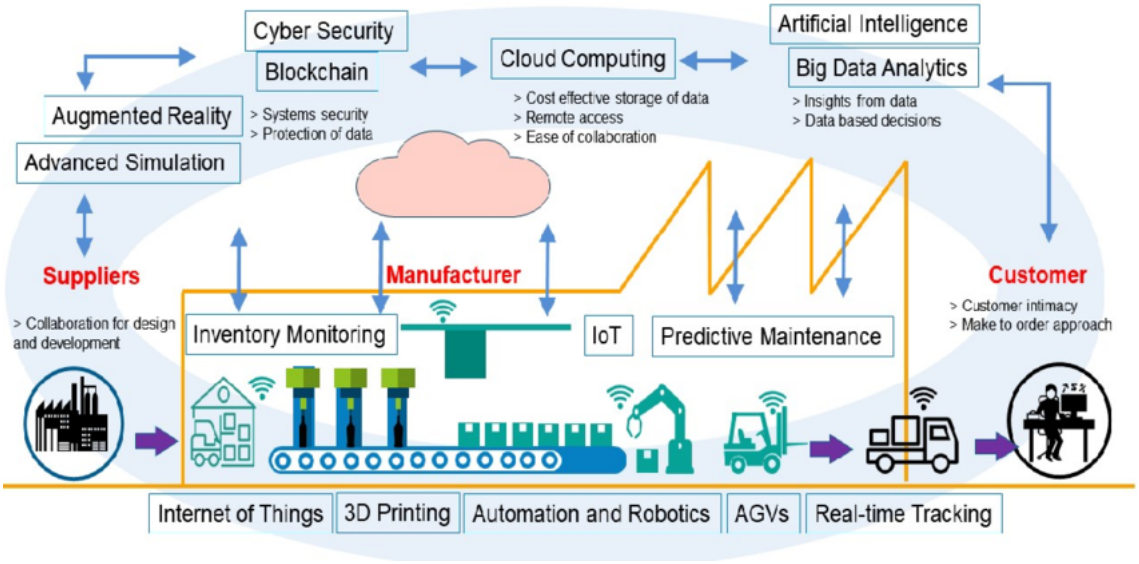


Figura 2.2 – Interconexão de tecnologias emergentes na indústria 4.0. Fonte: Adaptado de ResearchGate (MISHRA; MOHANTA; MAHANTY, 2022).

### 2.3.5 Tecnologia Blockchain

*Blockchain* é uma termo central que descreve o conceito inovador de distribuição de registros, cuja popularidade inicial veio de aplicações como criptomoedas (NAKAMOTO, 2008). A *blockchain* consiste em registros sequenciais, representados por blocos, que são conectados através de criptografia. A principal razão para a ampla adoção da *blockchain* é sua capacidade de revolucionar a maneira como as transações e a autenticação são realizadas de forma constante e eficiente. Ao romper com os métodos tradicionais e centralizados, a *blockchain* trouxe uma mudança radical, o que tem atraído grande aceitação pela comunidade industrial e empresarial (BODKHE et al., 2020). É fundamental considerar que quatro fatores são fundamentais para o êxito da *blockchain*: descentralização, inalterabilidade, transparência e segurança (TEISSERENC; SEPASGOZAR, 2021). Em conjunto, esses elementos possibilitam um novo patamar de confiança e eficiência no processo. Portanto:

- Descentralização: a *blockchain* distribui autoridade por toda a rede mundial de computadores, ou nós, assim descentralizando o controle da rede. Todo nó possui seu próprio registro do bloco, o que significa que cada transação é duplicada por todos os outros. Isso é vital para quando um dos nós falha e é necessário garantir que nenhuma informação seja perdida. Como não há intermediários no processo, todos têm a garantia de que não haverá problemas na entrega, e o cliente também garante que o fornecedor receberá o seu pagamento. Dessa forma, a ausência de intermediários reduz o tempo de espera nas transações e diminui os custos, aumentando as margens de lucro nas vendas (YETIS; KARAKOSE; BAYGIN, 2022).

- Imutabilidade: a transação na *blockchain* não pode ser alterada. Isso significa que uma ação é criada quando é validada, um algoritmo torna o bloco à prova de atividades maliciosas e não há como apagá-lo sem uma chave raiz. Naturalmente, esse atributo é necessário onde a transparência e os processos complicados exigem que a informação seja transparente. Uma transação bancária, como acréscimo, nunca será eliminada. Em suma, a alteração teria de começar a ser feita no bloco 1, e isso é impossível de fazer na prática. Qualquer tentativa de alteração comprometeria toda a cadeia de blocos, tornando a imutabilidade especialmente atrativa para indústrias que dependem dela em auditorias e regulamentações (BOSCHI; POLLICE; BATOCCHIO, 2020).

- Transparência: na *blockchain*, todas as transações são rastreáveis, mesmo que as identidades dos participantes possam ser protegidas por pseudônimos. A clareza do procedimento possibilita a qualquer nó da rede examinar a procedência e o registro das transações, assegurando sua autenticidade. Isso proporciona um benefício considerável para as cadeias de abastecimento mundiais, uma vez que possibilita o rastreamento da procedência dos produtos em cada fase do processo, garantindo que a origem dos produtos seja segura até o destino (KHAN; BYUN; PARK, 2020).

- Segurança: a *blockchain* é inovadora devido à sua segurança. A fusão de criptografia sofisticada com mecanismos de consenso entre os nós de uma rede faz com que a tecnologia seja extremamente difícil de ser manipulada ou fraudada. Para salvaguardar o sistema de ameaças, como a duplicação de transações, a rede precisa conferir a transação antes de inseri-la na sequência. A resiliência oferecida pela descentralização também reduz a possibilidade de uma única falha, o que é aconselhável em cenários de elevada confiabilidade (TYAGI et al., 2023).

  A figura 2.3 mostra como uma transação é solicitada, validada e adicionada à cadeia de blocos. Primeiro, a transação é criada e enviada para todos os nós da rede. Com uma infraestrutura à disposição, os nós, posteriormente, procuram validá-la usando um mecanismo de consenso chamado *proof of work* e, como recompensa, gerar algum valor que comprove 'trabalho'. Após ser validada, a transação será incluída em um novo bloco, ou bloco subsequente, o qual é então incorporado à *blockchain* e fica imutável para sempre. Estes cinco passos garantem a integridade, a transparência e a descentralização, as três características fundamentais da *blockchain*.

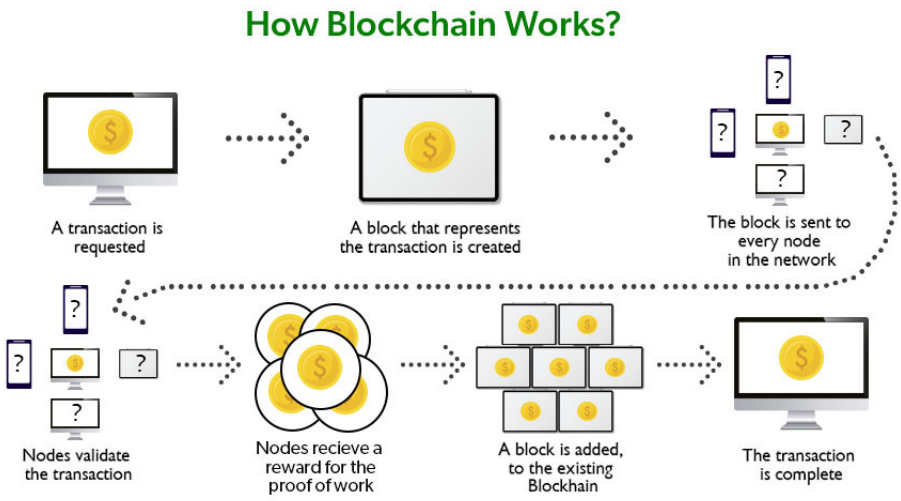


Figura 2.3 – Processo de funcionamento de uma *blockchain*, desde a solicitação de uma transação até a validação e sua inclusão no bloco final. Fonte: Adaptado de GeeksforGeeks (GeeksforGeeks, 2024b).

## 2.4 Impactos da Blockchain na Indústria

A tecnologia *blockchain* possui a capacidade de transformar drasticamente diversos setores econômicos. Ademais, nos anos recentes, seu papel tem ganhado destaque na construção da indústria 4.0. A *blockchain*, como um sistema de registro distribuído, descentralizado e transparente com proteção contra fraudes, agiliza economia em setores onde a centralização do poder é inaceitável para rastreabilidade, confiabilidade de dados e automatização de processos (BODKHE et al., 2020). Na próxima seção, são analisadas várias formas de uso da *blockchain*.

### 2.4.1 Cadeias de Suprimentos e Logística

A cadeia de suprimentos é uma das partes da indústria em que a *blockchain* mais se destaca. Uma revisão das cadeias de abastecimento modernas revela a presença de muitos intermediários e processos descentralizados. Em tal ambiente, administrar a rastreabilidade de cada produto e garantir a autenticidade de cada etapa é susceptível de erros significativos. Ao registrar todas e cada uma das etapas em um *distributed ledger*, cada parte interessada pode rastrear cada item do início ao fim. Exemplos:

- O Walmart, juntamente com a IBM, recorreu à *blockchain* para rastrear alimentos frescos desde as fazendas até a prateleira (KHAN; BYUN; PARK, 2020). Com a ajuda do IBM Food Trust, a *blockchain* permite que o Walmart identifique a origem de um produto alimentar em apenas alguns segundos no caso de contaminação. Isso melhora significativamente a segurança alimentar e a transparência para os consumidores.

- De Beers, conseguiu adotar a tecnologia *blockchain* rastreando a jornada de suas pedras preciosas, desde a atividade de mineração até o momento em que chegam ao consumidor final. A plataforma, conhecida como Tracr, ajuda os compradores a estabelecer a autenticidade de cada diamante de forma segura, sem chance de risco no comércio ilegal de diamantes, garantindo uma melhor transferência ao longo de toda a cadeia de valor.

Na figura 2.4.1, a integração de tecnologias emergentes como *blockchain* e IoT está presente na cadeia de suprimentos. Todos os envolvidos, desde o produtor até o consumidor final, têm acesso a uma base de dados distribuída que permite verificar regularmente o status dos produtos. Dessa forma, a autenticação e transparência está garantida na cadeia de suprimentos; o produto é rastreado digitalmente e de modo mais seguro. Os contratos inteligentes apoiam efetivamente a transferência de dados e valores de modo seguro e confiável; isso é vital para a indústria 4.0.

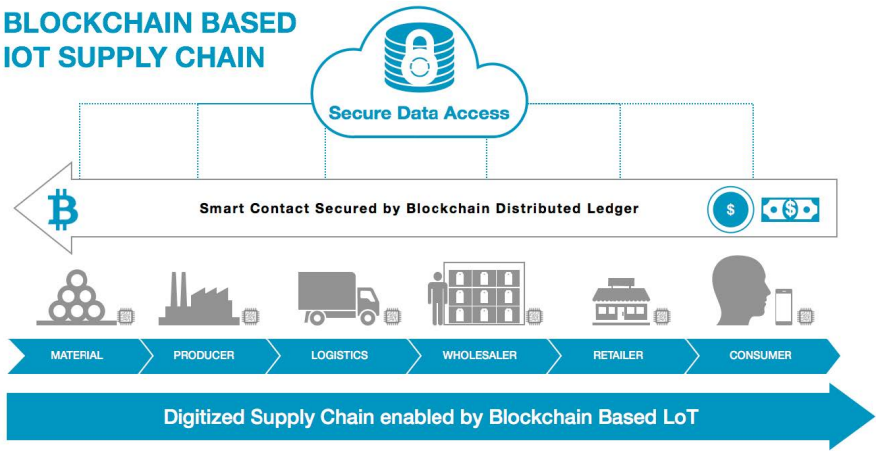


Figura 2.4 – Interconexão de tecnologias emergentes na indústria 4.0. Fonte: Adaptado de IoTHub (IoTHub, 2024).

### 2.4.2 Manufatura Inteligente

A manufatura inteligente, inovação em torno da qual a quarta Revolução Industrial é construída, já aproveita a avançada tecnologia de IoT, inteligência artificial e automação. No entanto, inovar também advém com desafios igualmente novos, como autenticidade, conformidade regulatória e rastreabilidade de peças. A complexidade da cadeia de fornecimento moderna – frequentemente uma rede de muitos fornecedores de várias partes do mundo – significa que é extremamente difícil garantir a rastreabilidade e autenticidade de qualquer peça.

Uma *blockchain* é a abordagem ideal, uma vez que fornecem o registro decente; auditável e imutável que permite a localização de cada peça e componente de um produto ao longo do abastecimento e produção corrente. Além de melhorar esse aspecto, ajuda a garantir a qualidade de peças e componentes verdadeiros ao longo do seu ciclo, o que é vital em numerosas indústrias, como a automotiva e a de aviação, onde a diferença de qualidade pode ser uma questão de vida ou

morte. Ademais, sensores de IoT podem ser integrados para monitorar automaticamente dados de produção, então postos na *blockchain* em tempo real, assim, aumentando a autenticação e redução da necessidade de intervenção humana (MOURTZIS; ANGELOPOULOS; PANOPOULOS, 2023). Exemplos:

- Volkswagen usa a *blockchain* da VeChain para garantir a autenticidade de *software* dos veículos e que não houve adulteração. Também usa a tecnologia para rastrear peças no processo de manufatura, assegurando que peças falsas não entrem na sua linha de produção.
- A Boeing, na aviação, por exemplo, está testando como pode usar a *blockchain* para rastrear peças de aeronaves, garantindo que sejam autenticas e respeitem os níveis de segurança necessários. Isto reduz o risco de falhas catastróficas e aumenta a confiabilidade da indústria.

A figura 2.4.2 ilustra como a *blockchain* e a IoT podem ser integradas na manufatura inteligente pela remota vigilância em tempo real da produção do respectivo objeto. Tecnologias de sensores IoT, por exemplo, monitoram os dados operacionais durante a manufatura e a inscrevem propriedade na *blockchain*. Dessa maneira, a autenticidade e a proveniência do metal das turbinas podem ser testadas e aprovadas. Tal nível de automação e vigilância em tempo real garantirá que apenas peças seguras serão empregadas na produção, melhorando a eficiência e mitigando os riscos e danos para o site de produção em casos críticos, tal como na indústria automotiva ou aviação.

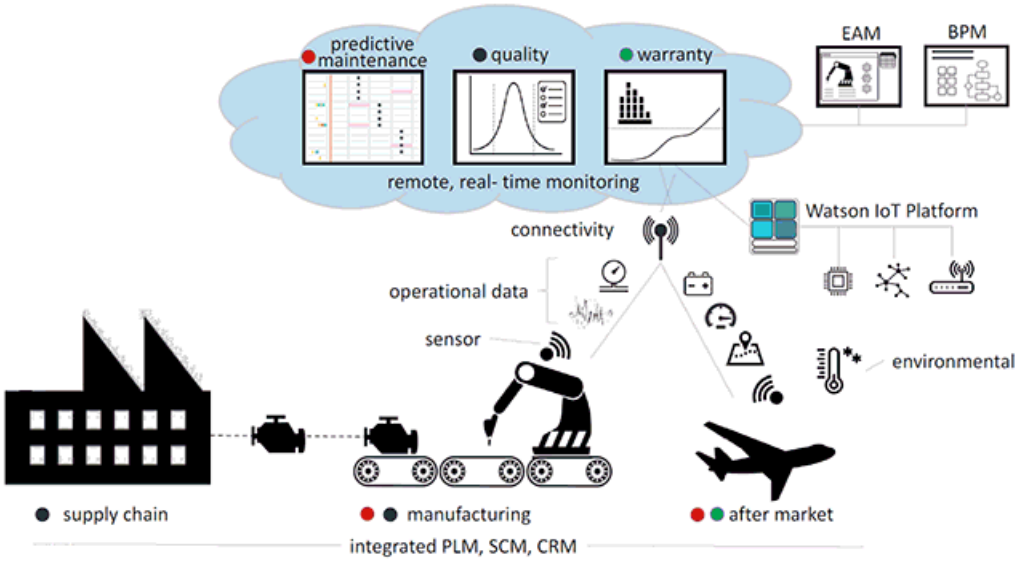


Figura 2.5 – Integração da *blockchain* e IoT na manufatura inteligente com monitoramento em tempo real. Fonte: Adaptado de Altoros (Altoros, 2024).

### 2.4.3 Comércio de Energia

Com o crescimento da integração de recursos energéticos renováveis e a geração cada vez mais descentralizada, até há pouco tempo, a energia era produzida por empresas de serviços públicos, que eram verticais em todo o ciclo – da eletricidade gerada até a distribuição, no entanto a emergência de *prosumers* levou à compreensão da necessidade de um ambiente energético descentralizado (EL-DIN et al., 2024). Um *prosumer* é um consumidor que produz energia enquanto a consome. Isso ocorre uma vez que ele também produz eletricidade por meio de algum sistema como um painel solar ao consumi-la.

A plataforma *blockchain* facilita a existência de mercados de energia descentralizados, em que o comprador pode adquirir energia do vendedor diretamente sem intermediários, como as gigantescas concessionárias. Isto se torna possível por meio dos contratos inteligentes, que permitem a negociação e faturamento automático mediante algum tipo de parâmetros, como a quantidade de energia produzida ou consumida. Isso diminui a taxa de transação e incentiva a propagação de fontes de energia limpa, visto que os consumidores podem gastar mais dinheiro na aquisição de energia gerada localmente. Além disso, a *blockchain* garante transações seguras entre as partes, já que elas não podem ser fraudadas e trazem mais confiança para o processo. Exemplos:

- O Projeto Brooklyn Microgrid possibilita aos habitantes locais com painéis solares vender sua produção excedente de eletricidade aos residentes nas redondezas via contrato inteligente, baseado na *blockchain*. Isso envolve o comércio de pequena escala de energia e diminui a taxa de dependência das concessionárias, enquanto também diminui a pressão sobre as fontes de flutuação.
- A plataforma WePower permite à corporação comprar de fontes de energia renovável diretamente via através de tokens da *blockchain* que representam a quantidade de eletricidade na qual o comprador irá investir. Isso simplifica o processo de compra e, além disso, auxilia no financiamento da instalação de novas fontes de energia limpa.

### 2.4.4 Indústria Farmacêutica e Saúde

O setor farmacêutico é uma indústria regulamentada ao extremo que é altamente desafiadora ao mesmo tempo. Por um lado, os produtos farmacêuticos apresentam uma ameaça de falsificação; por outro lado, há um desafio de rastrear todos os produtos compostos redundantes na cadeia de suprimentos, afetando as capacidades do consumidor e a saúde e a proteção do paciente. Portanto, no que diz respeito à falsificação, trata-se de um conceito crescente e em expansão, certamente mais aparente nos mercados emergentes e de terceiro mundo, onde a segurança e a proteção são menos altamente regulamentadas. Além disso, as cadeias de produção de empresa neste setor são frequentemente globais, tornando a troca global e transfronteiriça imensamente complicada na garantia da qualidade (KHAN; BYUN; PARK, 2020).

A *blockchain*, neste caso, é responsável por fornecer rastreabilidade total para medicamentos, desde a origem dos ingredientes até a entrega ao cliente final. Cada etapa é registrada de forma imutável, e as autoridades regulatórias e os cidadãos sabem a autenticidade do produto. Adicionalmente, na esfera da saúde, a *blockchain* pode ser usada para armazenar e compartilhar seguramente papeletas médicas, assegurando que os dados só possam ser acessados por pessoas autorizadas, e com isso prevenir a fraude e falsificação. Por exemplo:

- A plataforma MediLedger é outra maneira como grandes corporações farmacêuticas, incluindo Pfizer e Genentech, usam a *blockchain* para verificar medicamentos, garantindo que os medicamentos sejam genuínos. Sistemas baseados em *blockchain* garantem a autenticidade dos remédios e minimizam a falsificação na produção de medicamentos, garantindo a sua qualidade.

### 2.4.5 Seguros

A indústria de seguros possui uma forte presença de processos burocráticos, brechas conseguintes em ineficiências e longos períodos de liquidação de sinistros. A fraude e as disputas sob as condições das políticas são recorrentes, e custam a operadora dinheiro e arruínam a satisfação do consumidor. Na maioria das vezes, o processo de verificação e análise manual envolvido no pagamento do sinistro atrasa a liquidação, fazendo com que consumidores individuais se sintam desconfiados do campo. Adicionalmente, investigar um sinistro pode exigir um extenso envolvimento de terceiros e decisões que se tornem caras e demoradas para a companhia e os consumidores.

Uma solução pode ser integrar a *blockchain* em combinação com contratos inteligentes. Esses contratos podem, por sua vez, ser programados para executar o pagamento de uma apólice de seguro assumindo princípios indiscutíveis (BUTERIN et al., 2014). Portanto, no caso de um evento ocorrer, como um atraso em um voo ou desastres naturais, o pagamento será arcado, e não haverá necessidade de intervenção humana, reduzindo drasticamente o tempo de liquidação e os custos. A natureza imutável da *blockchain* garante que a política acordada não pode ser modificada, reduzindo também as disputas. Exemplos:

- A AXA, gigante do setor de seguros, desenvolveu o Fizzy, um seguro de voo automatizado que paga automaticamente quando um voo está atrasado por mais de duas horas, sem a necessidade de solicitação do cliente. Esse processo é garantido por contratos inteligentes baseados em *blockchain*.

- A Etherisc oferece seguros contra desastres naturais, onde os pagamentos são acionados automaticamente com base em dados meteorológicos verificados por contratos inteligentes, agilizando o processo de sinistros e reduzindo a chance de fraudes.

### 2.4.6 Setor Público e Governança

Desde a invenção do setor público, as pessoas sempre o associaram a uma enorme quantidade de burocracia, falta de transparência e prestações fraudulentas a cidadãos inocentes. Seja na emissão de todos os tipos de documentos oficiais, na organização de eleições justas ou simplesmente na manutenção de todos os tipos de registros públicos, o setor público sempre foi manchado por corrupção, vazamento público de informações pessoais, ou simplesmente práticas ineficazes, para todos os efeitos, o setor público é uma das fraquezas críticas da sociedade.

A *blockchain* surge como uma solução ideal, pois pode ser uma maneira perfeita para o setor público abordar todos os problemas associados à corrupção. Portanto, deve-se reconhecer o papel-chave que a *blockchain* desempenha no setor público, já que esta tecnologia é transparente, segura e descentralizada para processos vulneráveis. Os governos poderão empregá-lo para gerir registros públicos, como certidões de nascimento, registro de propriedade e licenças comerciais. Os registros seriam à prova de alterações e teriam de ser auditados minimalmente (BODKHE et al., 2020). Governos também poderiam utilizar *blockchain* para proteger votos de manipulações ou modificações. Dessa forma, votos podem ser verificados por todas as partes interessadas, tornando o sistema de votação suficientemente transparente e acessível. Além disso, cidadãos poderiam facilmente votar de casa, conforme a *blockchain* pode assegurar a segurança do processo (TYAGI et al., 2023). Exemplos :

- A Estônia usa *blockchain* para garantir a integridade das eleições eletrônicas , permitindo que os cidadãos votem remotamente de mancira segura e auditavel, eliminando a possibilidado de manipulação de votos.
- O governo dos Emirados Árabes Unidos está digitalizando e descentralizando serviços públicos, como emissão de licenças e registros de propriedade, com a meta de se tornar um dos primeiros países totalmente baseados em *blockchain* até 2025.

### 2.4.7 Componentes Chave da Blockchain:

Os blocos na *blockchain* são a principal unidade de acomodação e validação de transações e, assim, atuam como blocos de construção do desenvolvimento e funcionamento dessas tecnologias. Eles contêm informações cruciais para as tarefas vitais, garantindo a solidez do sistema com essa arquitetura embutido, já que quaisquer revelações são registradas e deduzidas com a capacidade imutável e segura. Portanto, esses elementos são vitais para o funcionamento adequado da *blockchain*, bem como para proporcionar segurança e proteção à prova de adulteração para os aplicativos empregados no setor industrial.

1. Cabeçalho do Bloco:

   O cabeçalho do bloco armazena os metadados que identificam o bloco e o vinculam ao anterior, garantindo a segurança e integridade.

- *Hash* do Bloco Anterior: esse campo é usado para armazenar o *hash* criptográfico do bloco anterior, fornecendo uma conexão ao bloco atual, formando assim uma cadeia contínua. Essa cadeia garante que, em tentativas de hackear para modificar dados de um bloco anterior, por exemplo, tal ação seria imediatamente detectada, uma vez que as alterações precisariam de uma recriação do *hash*, anulando todos os blocos subsequentes. Essa interligação entre blocos é fundamental para a imutabilidade da *blockchain*.
- Merkle Root: é o *hash* que condensa todas as transações que ocorreram dentro do bloco. Isso é conseguido por meio de uma árvore de Merkle; a árvore de Merkle é uma transformação usada para garantir que é possível verificar se quaisquer transações dentro do bloco foram alteradas. Em uma configuração industrial em que uma casualidade de transações está acontecendo, a Merkle root permite verificar a fidelidade das transações ao invés de vasculhar tudo. Isso aumenta a eficácia e garante que qualquer transação que tenha sido modificada seja identificada.
- Timestamp: é o responsável por registrar a data e hora em que o bloco foi criado. Os blocos são, em seguida, ordenados por carimbos de data e tempo. O tempo é crucial em aplicativos industriais que precisam ser auditáveis; por exemplo, no envio industrial e na rastreabilidade, um tempo exato de execução de uma transação ou evento é crítico.
- Nonce: um campo que contém um valor numérico, e esse valor é usado por mineradores para mesclar-se com outras transações dentro de um bloco até que resulte em um *hash* que satisfaça a dificuldade estabelecida pela rede. No algoritmo de consenso *proof of work* (PoW), encontrar o nonce correto é um processo intensivo em termos de poder computacional, mas é essa dificuldade que garante a segurança da rede, impedindo ataques e manipulações.
- Versão do Bloco: Esse campo indica a versão do protocolo da *blockchain* utilizado na criação do bloco. Isso garante que as atualizações do protocolo possam ser implementadas de forma retrocompatível, permitindo a evolução da rede sem comprometer a integridade dos blocos anteriores.

2. Corpo do Bloco:

   O corpo do bloco contém as transações verificadas que são permanentemente registradas na *blockchain*. Cada transação é validada pelos nós da rede antes de ser incluída no bloco.

   - Transações: O “corpo” ou bloco propriamente dito, é composto por um conjunto validado de transações. Essas transações podem abranger, desde a troca de ativos digitais até a execução de contratos inteligentes. No caso da indústria 4.0, podem englobar desde o envio de mercadorias, a execução de contratos de abastecimento automaticamente, ou ainda o registo de dados, vindo de sensores IoT que monitoram

o desempenho de maquinaria. Desta forma, ao assegurar que todas as transações sejam imutáveis e verificáveis, a *blockchain* ao induzir um nível de confiança e de segurança complementar, exige a confiança e a segurança necessárias em ambientes industriais robotizados.

A figura 2.6 demonstra a estrutura dos blocos em uma *blockchain*, destacando a forma como os blocos são encadeados, desde o bloco anterior até o bloco subsequente. O cabeçalho de cada bloco inclui informações necessárias como o *hash* do bloco anterior, timestamp, raiz de Merkle, e muito mais, esse dado é importante para que se possa garantir a integridade e segurança de uma cadeia de blocos. Tal como mostra a figura abaixo, a obtenção de Merkle root de um provedor, trabalhando sob prova de trabalho, permite que os nós da rede validem e encadeiem blocos entre si , ao final, garantindo imutabilidade da cadeia.

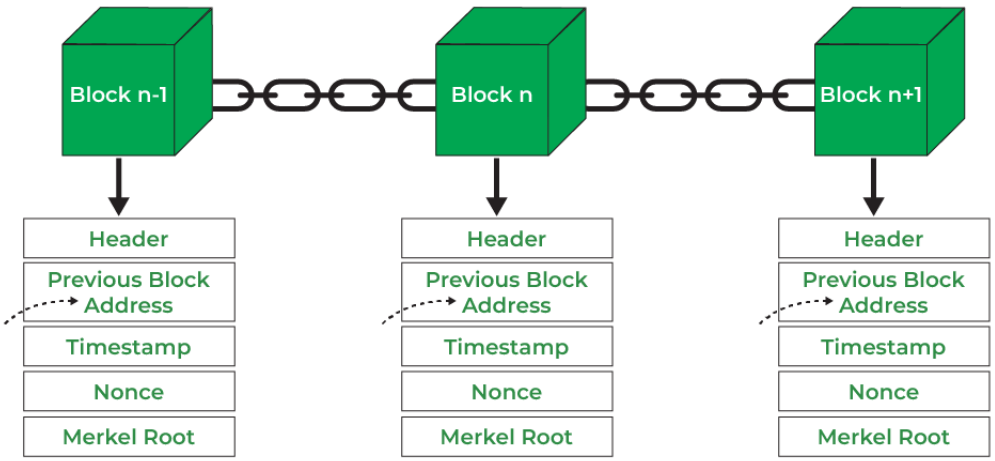


Figura 2.6 – Estrutura dos blocos em uma *blockchain*. Fonte: Adaptado de GeeksforGeeks (GeeksforGeeks, 2024a).

**Mecanismo de Hash**

Um *hash* é um método matemático que converte um dado em uma sequência específica de caracteres; normalmente em hexadecimal. Independentemente de o arquivo de dados ser pequeno ou grande, ele será expresso em um código único. O *hash* é um recurso essencial para a segurança em diversas áreas da cibersegurança.

Na *blockchain*, os hashes servem para:

- Ligar blocos entre si: cada bloco na *blockchain* contém o *hash* criptográfico do bloco anterior, criando uma cadeia contínua de blocos. Essa ligação entre os blocos garante que qualquer alteração em um bloco anterior resultará na modificação do *hash*, quebrando a cadeia e invalidando todos os blocos subsequentes. Isso torna a *blockchain* imutável e resistente a tentativas de adulteração.

- Integridade dos dados: o *hash* é uma função determinística, o que significa que uma mínima mudança na entrada de dados resulta em um *hash* completamente distinto. Isso permite à rede verificar a integridade das transações e blocos. Se algum dos dados em um bloco for alterado, o *hash* resultante da mudança não corresponderá ao armazenado, e o bloco será invalidado.

- Proteger contra fraudes e adulterações: outra característica da *blockchain* é que ela é segura contra fraudes e adulterações. Devido ao *hash*, um *blockchain* é extremamente seguro contra fraudes. Isso ocorre porque mudar um bloco significa modificar e reconstruir todos os blocos subsequentes. Em uma rede distribuída, uma tentativa como essa seria imediatamente detectada, o que significa que um invasor não pode alterar nenhum bloco sem ser imediatamente reconhecido.

  O mecanismo de *hash* torna a *blockchain* confiável para assuntos de integridade e segurança. Isso torna a tecnologia *blockchain* adequada para usos que requerem alto nível de segurança, como transações bancárias, contratos inteligentes e produtos de rastreamento na cadeia de fornecimento.

## 2.5 Algoritmos de Consenso

Os algoritmos de consenso são protocolos essenciais para a operação de sistemas distribuídos, como as redes *blockchain*. Eles garantem que todos os participantes (ou nós) de uma rede distribuída concordem sobre o estado atual do sistema, mesmo na presença de falhas e atores maliciosos. O consenso é um desafio fundamental em sistemas distribuídos devido à necessidade de coordenação entre nós que podem não confiar uns nos outros e que podem ter visões inconsistentes do estado da rede (LAMPORT; SHOSTAK; PEASE, 1982).

Os algoritmos de consenso são vitais para a descentralização e a segurança das redes *blockchain*, pois evitam a necessidade de uma autoridade central para validar e registrar transações. Em vez disso, a rede como um todo trabalha para validar transações de maneira colaborativa e segura. Este processo garante que todos os nós mantenham uma cópia consistente da *blockchain*, impedindo a ocorrência de problemas como o "gasto duplo" (*double spending*) (NAKAMOTO, 2008).

Existem vários algoritmos de consenso, cada um com suas próprias vantagens e desvantagens, adaptando-se a diferentes requisitos e cenários de uso. Os principais algoritmos de consenso incluem:

### 2.5.1 Proof of Work (PoW)

**Funcionamento**

*Proof of Work* é um algoritmo de consenso estabelecido, originalmente introduzido no Bitcoin (NAKAMOTO, 2008). No PoW, os mineradores competem para resolver complexos problemas matemáticos criptográficos usando funções de *hash*. O *Secure Hash Algorithm* é o algoritmo de 256 bits usado no Bitcoin (SHA-256). Desde que começou a exploração de criptomoedas, tornou-se uma prática padrão usar o SHA-256 para as operações de mineração. O minerador se esforça para encontrar um *nonce* – um número arbitrário – tal que o valor de *hash* do bloco de dados concatenado com o *nonce* satisfaça um requerimento específico. Tipicamente, a rede exige que o valor de *hash* comece com n zeros. Este processo depende da probabilidade, sendo necessário experimentar várias opções. Além disso, a adaptação da complexidade é um parâmetro fundamental no PoW. Como o número de processadores na rede é desconhecido, o requisito de descendência não ajustável pode torná-lo muito lento para alguns blocos e muito rápido para outros. Assim que o requisito for encontrado, o minerador transmite a nova estrutura para a rede para poder ser verificada.

**Segurança**

O PoW é seguro devido ao enorme poder computacional necessário para manipular a *blockchain*. O chamado ataque de 51% exigiria do invasor que ele ou ela controlasse mais poder computacional do que a soma de todos os outros mineradores da rede (NAKAMOTO, 2008). Desta forma, seria possível reescrever partes da *blockchain* e até realizar ataques duplos. No entanto, o esforço computacional e energético necessário para obter esse controle seria virtualmente impossível para a maioria em termos de viabilidade econômica. Além disso, a imutabilidade dos blocos anteriores é garantida pela função de *hash*, que vincula criptograficamente cada bloco ao anterior. Isso significa que modificar um bloco já inserido na cadeia exigiria recalcular todos os blocos subsequentes, o que aumentaria ainda mais os custos computacionais de um ataque. Portanto, o PoW, além de ser robusto, aproveita o fato de que a segurança da rede depende diretamente dos recursos necessários para gerar e validar novos blocos.

### 2.5.2 Proof of Stake (PoS)

**Funcionamento**

A *proof of stake* é uma alternativa ao PoW. O Peercoin (KING; NADAL, 2012) propôs a PoS para escolher validadores para a proposta de novos blocos, baseando-se na quantidade de criptomoedas que eles possuem e na disposição para "apostar" na garantia. A escolha dos validadores é pseudo-aleatória, considerando a quantidade de criptomoedas em *stake* e, em alguns casos, a idade da moeda, também chamada de "*coin age*". Assim, em vez dos validadores competirem entre si para resolver problemas matemáticos como no PoW, são escolhidos para propor blocos e validar transações com base na quantidade de moedas que possuem em *stake*. Se um validador tentar adicionar um bloco inválido, perde as moedas que apostou, o que o encoraja a se comportar adequadamente (BENTOV et al., 2014). Ademais, a *proof of stake* é mais sustentável por ter menos gasto energético.

#### Segurança

O PoS é mais eficaz no uso de energia do que o PoW, e torna economicamente inviável para um atacante adquirir uma participação significativa na rede. A razão pela qual tal invasão é realmente impossível, no entanto, é que o PoS não se baseia no poder computacional, ou seja, um invasor precisaria comprar um número absurdo de moedas, que teria um custo proibitivo. A proteção do PoS está fortemente atrelada à distribuição de criptomoedas entre os participantes da rede. Se um pequeno número de indivíduos possui uma fração muito grande das moedas, a rede pode ser invadida (PAVLOFF; AMOUSSOU-GUENOU; TUCCI-PIERGIOVANNI, 2022).

### 2.5.3 Delegated Proof of Stake (DPoS)

#### Funcionamento

*Delegated proof of stake* foi criado por Daniel Larimer (LARIMER, 2014) e é adotado por blocos como BitShares, Steemit e EOS. No DPoS, os titulares de tokens votam em um conjunto fixo de delegados e testemunhas , que são responsáveis por validar transações e minerar blocos. Os delegados são eleitos por um sistema de votação de rito consagrado, no qual os titulares de tokens são capazes de alterar os votos a qualquer momento. Isso reforça a natureza democrática da autoridade, uma vez que os delegados eleitos devem se sustentar no poder para buscar a aprovação da comunidade. Este modelo também fornece uma saída para garantir autonomia em situações cotidianas ou extraordinárias. Tal abordagem, no entanto, também é considerada uma desvantagem em termos de segurança, pois o mecanismo mais eficiente de DPoS, que fornece criatividade e inovação, é centralizado, e pode levar ao fornecimento de equipamentos com quantidade limitada de validadores, o que não é natural, pois concentra o poder de decisão em poucas mãos.

#### Segurança

A maior eficiência desse algoritmo se deve à sua concentração de validadores, o que melhora o desempenho e a capacidade do sistema, já que o número reduzido de validadores cria oportunidades para processamento de transações em um curto período. No entanto, isso também é tambem causa um efeito negativo, porque o nível de descentralização no sistema é reduzido. Por causa da necessidade de apenas um ou dois validadores, pode-se encontrar manipulações do grupo de ataque, que prejudicam o plano de sistemas (GAI; QIU; SUN, 2017).

#### Algoritmos alternativos

Além desses, existem outros algoritmos de consenso emergentes e híbridos, como *proof of authority* (PoA), *byzantine fault tolerance* (BFT) e suas variantes, que buscam otimizar diferentes aspectos como escalabilidade, segurança e eficiência energética.

## 2.6 Aplicações de blockchain na indústria 4.0

Entre os componentes da era da indústria 4.0, está a tecnologia *blockchain*, considerada crítica. Seus benefícios vão além da automação, estendendo-se á descentralização, imutabilidade e transparência. Essa tecnologia abre oportunidades em áreas críticas, como segurança de dados, confiabilidade das cadeias de suprimento e valor. No caso de uma indústria que se torna cada vez mais descentralizada e em rede, *blockchain* permite um nível completamente novo de confiança e capacitação, tornando-se um elo interno mais seguro, auditável e autônomo para integrar sistemas e informações. É uma fonte de transparência e controle, mesmo em um processo extremamente complexo, e permite a construção de um novo modelo de negócio, vagamente vinculado ao modelo de governança menos centralizado e mais transparente.

#### 2.6.0.1 Rastreabilidade de cadeia de suprimentos

A melhor parte da contribuição da *blockchain* para a cadeia de suprimentos não é apenas o rastreamento: é revolucionário criar uma riqueza de dados disponíveis de fontes independentes confiáveis, tudo sem a necessidade de um intermediário. A razão é que a *blockchain* não apenas promove a riqueza dos dados, mas promove as auditorias imparciais com seus livros públicos disponíveis (BOSCHI; POLLICE; BATOCCHIO, 2020). Seus livros públicos eliminam a necessidade de auditoria centralizada levando ao aumento da frequência das auditorias e a diminuição do custo total para todos que participam. Com a *blockchain* na logística, o rastreamento de itens não é um grande problema, mas, mais importante ainda, é a maneira como isso se traduz em interoperabilidade entre diferentes sistemas. A tecnologia realmente permite a interoperabilidade entre diferentes sistemas de várias empresas e regiões. Este é um excelente exemplo para os casos de uso de negócios. Quando se trata de cadeias de fornecimento complexas e globais com várias partes interessadas, a desconfiança entre essas pessoas pode ser um problema. Aqui, a *blockchain* serve como uma camada de confiança entre elas e todas as partes; a negociação é registrada permanentemente e acessível a todas partes, e os intermediários não são necessários.

Na figura 2.6.0.1, é exposto como a *blockchain* contribui para o processo de cadeia de suprimentos. Proporciona-se mais clareza, rastreabilidade e confiabilidade em cada etapa, desde os fornecedores até os consumidores finais. Além disso, a tecnologia *blockchain* facilita a administração do padrão de qualidade, possibilita a interligação dos sistemas e elimina intermediários, diminuindo custos e maximizando a eficiência das auditorias (YETIS; KARAKOSE; BAYGIN, 2022).

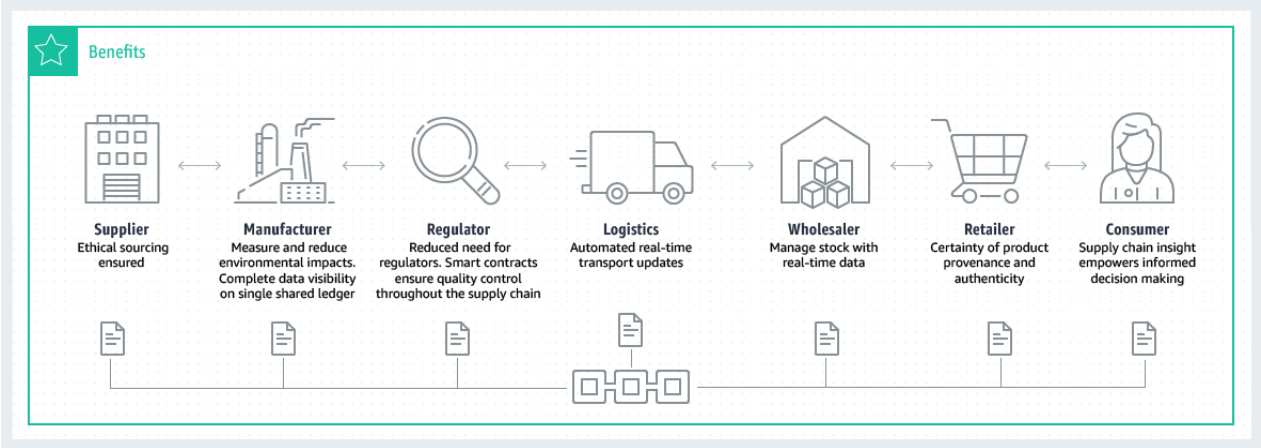


Figura 2.7 – Benefícios da *blockchain* na cadeia de suprimentos. Fonte: Adaptado de AWS (Amazon Web Services, 2024).

#### 2.6.0.2 Smart contracts (contratos inteligentes)

Os *smart contracts* (contratos inteligentes) são softwares autoexecutáveis que operam na *blockchain* e, quando as condições são atendidas, processam transações com as partes interessadas. Essa tecnologia transforma qualquer processo comercial em 100% automático, removendo o elo intermediário e transmitindo o procedimento de uma maneira clara e segura (BUTERIN et al., 2014). Sua principal aplicação é a conclusão e implementação de acordos no âmbito descentralizado. Um *smart contract* pouco se assemelha a um contrato normal; no entanto, o software traduz diretamente o acordo em ação e assegura que o contrato seja cumprido sem compromissos em uma terceira administração. Portanto, o risco de contenda e fraude é muito baixo, já que todos os eventos e transações são armazenados para sempre e não podem ser alteradas. Um dos exemplos mais imediatos é a cadeia de fornecimento. O IoT garantirá a condição da mercadoria e efetuará o pagamento. Outros exemplos são contratos de manutenção em que a condição é monitorada, pelo sensor IoT, e a realização serve como métrica para pagamento (KHAN; BYUN; PARK, 2020).

Apesar do enorme potencial, porém, os *smart contracts* ainda enfrentam desafios, o mais significativo dos quais é a segurança. Uma vez que foi programado, executa o contrato exatamente conforme a descrição do código, tornando-o passível à exploração por erro ou falha de programação. Um dos exemplos mais notórios é o ataque à *Decentralized Autonomous Organization* em 2016, quando uma falha no código do contrato permitiu a um atacante desviar milhões de dólares em Ether (SIEGEL, 2016). A experiência deixou claro a necessidade de verificar código de *smart contracts* antes de sua aplicação em um ambiente real e onde são necessários.

Além desses, a segurança normativa constitui um outro desafio, dada a incerteza da validade do contrato inteligente em jurisdições variadas. No entanto, conforme a tecnologia se

desenvolve, podemos esperar para superar esses desafios à medida que os *smart contracts* se tornem uma parte vital de todo processo industrial e comercial (SZABO, 1997).

A figura 2.6.0.2 ilustra as etapas do funcionamento de um *smart contract* (contrato inteligente) na *blockchain*. O processo começa com a identificação das partes e o estabelecimento dos termos, seguido pela definição das condições. Após a implementação, o contrato é executado automaticamente quando as condições estabelecidas são atendidas. Por fim, as modificações são registradas em todos os pontos da rede, garantindo a imutabilidade e a transparência das operações.

Figura 2.8 – Etapas de funcionamento de um contrato inteligente na *blockchain*.

#### 2.6.0.3 Segurança de dados e privacidade

A segurança da *blockchain* não é restrita à mera proteção desses dados, é também questão de como essas informações são publicadas em cada um dos nós. Esse conceito é diretamente oposto a todas as formas tradicionais de controle centralizado, em que um único ponto de controle basta para permitir ou negar o acesso a uma fonte de dados, devido à autenticação centralizada e métricas de autorização. Na indústria 4.0, a *blockchain* se destaca, especialmente em redes IoT. Embora auditorias periódicas sejam comuns em sistemas tradicionais, a *blockchain* permite que os dados sejam autenticados e validados continuamente, sem a necessidade de uma autoridade central (BOSCHI; POLLICE; BATOCCHIO, 2020). Isso é crucial porque traz um novo valor genuíno para a área. Além disso, a tecnologia possibilita um alto grau de conformidade regulatória em setores altamente regulamentados, como saúde ou o setor automotivo.

#### 2.6.0.4 Manutenção preditiva

Por sua vez, a *blockchain* é uma das maneiras de validar os dados adquiridos dos sensores de IoT que monitoram a condição de máquinas e equipamentos em tempo real. Enquanto gravados em uma rede distribuída, esses dados são impossíveis de alterar. Ao mesmo tempo, a *blockchain* melhora a confiabilidade da previsão de falhas. Além disso, a *blockchain* pode simplificar e apoiar a entrada de dados dos sensores em sistemas de IA (inteligência artificial) que podem não só analisar o desempenho da máquina, mas também prever a possibilidade de falhas, tendo referido aos padrões de trabalho anterior (MOURTZIS; ANGELOPOULOS; PANOPOULOS, 2023).

O uso de *blockchain* em manutenção preditiva aprimora a confiança e a transparência também, já que, diferentemente dos sistemas tradicionais que podem ser manipulados, a *blockchain* torna qualquer adulteração de dados imediatamente rastreável. Com seus dados verificados, a *blockchain* promove a confiança nas previsões baseadas nesses dados e minimiza paradas inesperadas (KHAN; BYUN; PARK, 2020).

#### 2.6.0.5 Autenticação e combate à falsificação

Os setores onde a *blockchain* pode fornecer uma solução definitiva são farmacêutico e automotivo, onde a falsificação de produtos pode ser crítica. A finalidade da tecnologia *blockchain* é ter uma trilha de auditoria completa. Isso significa que cada etapa de um produto desde a produção até a entrega ao destinatário final pode ser verificada de forma transparente por todas as partes interessadas (BOSCHI; POLLICE; BATOCCHIO, 2020). Além disso, garante a integridade no processo de autenticação, uma vez que qualquer alteração resultaria em erro. Por outro lado, esta característica difere dos sistemas de rastreamento tradicionais que são mais fáceis de serem manipulados. No caso do setor farmacêutico, os medicamentos podem ser rastreados a fim de garantir que cada lote seja legítimo, ao mesmo tempo permitindo que os consumidores finais desenvolvam o hábito de verificar o que consomem.

### 2.6.1 Desafios e limitações

A figura 2.6.1 apresenta os desafios e limitações enfrentados na adoção da *blockchain* na cadeia de suprimentos. Esses desafios incluem a incerteza quanto à origem ética dos produtos por parte dos fornecedores, dificuldades dos fabricantes em monitorar impactos ambientais e perda de dados, controle de qualidade irregular pelos reguladores, falta de atualizações em tempo real na logística, além de problemas com superestoque e falta de estoque para atacadistas e incertezas na procedência dos produtos para os consumidores finais. Esses obstáculos precisam ser superados para uma implementação eficaz da *blockchain* na indústria 4.0 (MOURTZIS; ANGELOPOULOS; PANOPOULOS, 2023).

Figura 2.9 – Desafios e limitações da adoção da *blockchain* na cadeia de suprimentos. Fonte: Adaptado de AWS (Amazon Web Services, 2024).

#### 2.6.1.1 Escalabilidade

Em primeiro lugar, podemos mencionar que a escalabilidade continua sendo um dos maiores obstáculos para a aplicação da *blockchain* em indústrias. No momento, a *blockchain* fica limitada ao processamento de capacidade, o que significa que o número de transações que podem ser processadas por segundo fica muito atrás sistematicamente em comparação com as capacidades dos sistemas tradicionais centralizado. Isso pode resultar em uma redução na eficácia de sistemas de larga escala, como cadeias de suprimento globais, que têm a capacidade de suportar uma quantidade massiva de transações de processamento em favorecer a experiência. Uma possível solução para esse problema poderia ser o desenvolvimento de novos protocolos e melhorias de infraestrutura, especialmente usando *blockchains* privadas ou paralelas para espalhar os encargos de processamento (PAVLOFF; AMOUSSOU-GUENOU; TUCCI-PIERGIOVANNI, 2022).

#### 2.6.1.2 Custo e a complexidade

É possível discutir o custo e a complexidade de uma *blockchain*. A implementação de uma infraestrutura baseada em *blockchain* é acompanhada por custos e limites de *hardware* e *software*. Em primeiro lugar, especialmente para uma rede de um sistema descentralizado robusta, é necessária uma equipe de especialistas altamente preparada, o que pode aumentar os custos para todas as empresas que desejam se orientar para essa tecnologia (BODKHE et al., 2020). Manutenção de *software blockchain*, supervisão e outras atividades afins podem se tornar uma obrigação séria que requer capital intensivo, sendo esse um obstáculo para pequenas e médias empresas que dispõem de capital limitado e de conhecimento técnico suficiente para liderar e administrar esse significativo investimento.

#### 2.6.1.3 Interoperabilidade

Um desafio adicional é a interoperabilidade da *blockchain*, ou seja, a integração desta tecnologia com sistemas de TI legados e outras tecnologias emergentes da indústria 4.0, tais como a Internet das Coisas (IoT) e a inteligência artificial (TYAGI et al., 2023). Essa questão é particularmente complexa, uma vez que a tecnologia *blockchain* precisa ser incorporada a ecossistemas preexistentes. Muitas indústrias ainda empregam sistemas de TI obsoletos, incapazes de suportar diretamente a adoção da tecnologia *blockchain*. Além disso, a situação é agravada pela diversidade de padrões técnicos e regulatórios vigentes. Proporcionar a uma plataforma ou categoria de aplicação existente a capacidade de utilizar a *blockchain* requer um significativo esforço em pesquisa e desenvolvimento. É essencial garantir que os sistemas envolvidos possam se comunicar entre si, permitindo que tecnologias distintas troquem informações de forma eficiente. Frequentemente, isso implica no desenvolvimento de uma camada adicional de rede, posicionada acima das tecnologias existentes.

#### 2.6.1.4 Impacto Ambiental

Uma grande preocupação com a *blockchain* é seu impacto ambiental. A mineração de muitas *blockchains*, especialmente daquelas que usam o PoW, consome grandes quantidades de energia, criando uma pegada de carbono que cria problemas, especialmente quando a fonte de eletricidade é não-renovável. A transição para um futuro industrial sustentável requer abordagens energeticamente eficazes; desse modo, uma relutância em atualizar ou reformular a arquitetura das *blockchains* existentes pode se tornar um grande problema. Consequentemente, soluções como o PoS ou *blockchains* híbridos e energeticamente eficientes emergem (PAVLOFF; AMOUSSOU-GUENOU; TUCCI-PIERGIOVANNI, 2022).

#### 2.6.1.5 Tempo de Validação e Latência

Além da escalabilidade, o tempo de validação e a latência são problemas importantes, principalmente para setores que demandam respostas rápidas e transações em tempo real. O tempo de validação de transações e a latência no processo de consenso podem ser inadequados para ambientes que exigem decisões em milissegundos, como a automação industrial. Isso pode causar atrasos em processos críticos. Métodos como PoS e sidechains podem contribuir para superar esse obstáculo, aprimorando a performance da *blockchain* em contextos que demandam baixa latência. Uma sidechain é uma blockchain separada que opera de maneira paralela à blockchain principal (conhecida também como *mainchain*), permitindo a transferência de ativos entre as duas. As sidechains, conectadas à rede principal (conhecida também como *mainchain*), possibilitam a execução de transações fora da cadeia principal, acelerando o processamento e diminuindo a pressão na *blockchain* principal (BUTERIN et al., 2014).

#### 2.6.1.6 Segurança em Redes Híbridas

Devido sua estrutura descentralizada, a *blockchain* é considerada uma infraestrutura altamente segura. No entanto, no contexto das redes híbridas, sem dúvida, esse não é o caso, uma vez que a conexão entre os sistemas da *blockchain* e os sistemas de TI tradicionais é um dos principais pontos fracos por onde um *hacker* pode penetrar (MOURTZIS; ANGELOPOULOS; PANOPOULOS, 2023). Assim, ao combinar os sistemas, é essencial garantir a segurança nos pontos de conexão entre eles, onde a integração acontece, logo uma conexão sincronizada de serviços de segurança cibernética deve estar operacional para proteger informações pessoais e interromper métodos maliciosos de exploração de vulnerabilidades entre as tecnologias envolvidas.

#### 2.6.1.7 Governança Descentralizada

Do ponto de vista negativo, a governança descentralizada do *blockchain* pode ser facilmente considerada um desafio. Decisões em torno das redes *blockchain* são feitas por consenso, o que pode ser um processo moroso e complicado. Principalmente em *blockchains* públicas ou privadas com inúmeros participantes, podem ocorrer atrasos nas atualizações requeridas, discordância entre os participantes e até mesmo um impasse na direção da rede no futuro. Em cadeias de abastecimento globais, com diversos participantes envolvidos, essas podem ser barreiras intransponíveis para uma implementação eficiente e ágil (BOSCHI; POLLICE; BATOCCHIO, 2020).

#### 2.6.1.8 Privacidade dos Dados

No setor privado, a privacidade dos dados é uma prioridade na *blockchain*. Muitas plataformas que guardam dados de saúde utilizam uma *blockchain* privada, devido à sensibilidade e ao sigilo dos dados médicos (KHAN; BYUN; PARK, 2020). No entanto, a lei da União Europeia sobre proteção geral de dados, GDPR (European Parliament and Council of the European Union, 2016), impõe que os cidadãos têm o direito de excluir ou alterar seus dados; apresentando um desafio devido à natureza imutável da *blockchain*.

Uma solução é tecnologias como ZK-SNARKs (*zero-knowledge proofs*) (BEN-SASSON et al., 2014), o qual permite que uma parte (propositor) prove algo a outra sem revelar os dados. Isto garante privacidade, permitindo verificação sem expor informações pessoais, estando de acordo com regulamentos sobre privacidade, mas sem comprometer a segurança.

Em indústrias tais como fabricação e logística, onde os dados pessoais não são o foco, o desafio central é a segurança dos dados corporativos o asseguramento do controle de acesso e a integridade dos sistemas, sem a necessidade de seguir estritas regras de proteção de dados.

#### 2.6.1.9 Barreiras Culturais e Resistência à Mudança

Finalmente, a utilização da tecnologia *blockchain* enfrenta resistência cultural por parte das organizações. Em uma cultura tradicional, muitas empresas podem ser reticentes sobre tal tecnologia disruptiva, particularmente se não tem conhecimentos técnicos suficientes sobre como a *blockchain* é integrada em processos já existentes (MOURTZIS; ANGELOPOULOS; PANOPOULOS, 2023). A educação e a formação têm de ser incentivadas a fim de vencer essa resistência e assegurar que empresas tenham condições de implementar a operação da *blockchain* corretamente e com sucesso.

### 2.6.2 Conclusão

A *blockchain* é uma tecnologia inovadora e revolucionária que permite processos seguros, transparentes e automáticos. Onde quer que estejam envolvidos na indústria, seja na cadeia de fornecimento, produção ou transporte, os dados imutáveis e descentralizados são úteis. No entanto, várias questões técnicas, regulamentares e ambientais ainda existem para que ela se torne mais aceitável. É fundamental que questões de escalabilidade, interconectividade com os antigos e novos sistemas e latência devam ser resolvidas enquanto a *blockchain* se adapta para diminuir sua pegada de carbono. Mais um esforço necessário é criar infraestrutura de *blockchain* que seja acessível e fácil para as pequenas e médias empresas incorporarem e usarem (YETIS; KARAKOSE; BAYGIN, 2022).

A importância real é com a governança descentralizada e a proteção de dados, duas questões que exigem soluções complexas para garantir que não haja conflito e a conformidade regulatória seja atendida também. Cultura e resistência em uma organização são melhor resolvidas com treinamentos e conscientização para que as pessoas estejam plenamente preparadas para atender e trabalhar com o *blockchain* (MOURTZIS; ANGELOPOULOS; PANOPOULOS, 2023). À medida que a tecnologia subjacente evolui, esses serão problemas gradualmente superados conforme a *blockchain* se espalha efetivamente por mais setores da indústria. Só com uma implementação adequada conseguiremos promover um futuro brilhante para o *blockchain* na indústria 4.0.

# 3 Plataformas Blockchain

## 3.1 Introdução ao Ethereum

### 3.1.1 Conceito e Contextualização

No ano de 2015, Vitalik Buterin lançou o Ethereum, que foi um salto à frente em como o *blockchain* pode ser utilizado e posteriormente é continuação do protótipo que o Bitcoin havia começado (BUTERIN et al., 2014). Enquanto o Bitcoin se destina a ser uma moeda digital e um sistema de pagamento distribuído, este último é considerado como infraestrutura compartilhada para acordos automaticamente executados e aplicativos distribuídos. O Ethereum é blockchain onde é possível edificar e fazer funcionar esses contratos de forma segura e descentralizada (SZABO, 1997). Ocasionalmente, como esses contratos automatizam procedimentos e transações e eliminam o intermediário, eles também são mais baratos e mais eficazes de operar.

Digamos que você pode usar um contrato inteligente para transferir dinheiro de uma parte para outra após a conclusão de uma transação. Dessa forma, você economiza dinheiro em comissões de mediadores. No entanto, os contratos inteligentes são apenas uma parte do cenário com o Ethereum. Ele também permite a criação e execução de aplicativos descentralizados, frequentemente chamados de contratos inteligentes 2.0. Permite criar e executar aplicativos descentralizados, também conhecidos como contratos inteligentes 2.0. Esses aplicativos, funcionam na *blockchain* Ethereum, também são mais eficientes e baratos que seus análogos tradicionais. Isso porque, ao contrário dos aplicativos convencionais que dependem de servidores centrais e bancos de dados e, portanto, estão sujeitos a falhas no servidor ou no *frontend*, os dApps são livres de erros.

O Ethereum 2.0 é a rede atualizada para a adição de alterações significativas por meio de sua arquitetura. Este novo paradigma no ecossistema de *blockchain* ofereceu aumento de eficiência, segurança e, em última instância e em certos casos, da escalabilidade. A Ethereum 2.0 tem o PoS em vez do PoW. Isso reduz o consumo de energia e, ao mesmo tempo, a parte da escalabilidade do sistema. Por exemplo, *shards* são introduzidos. Dessa forma, *blockchain* é dividido em compartimentos e transações ocorrem enquanto contratos podem ser executados em paralelo. Isso aumenta a capacidade da rede.

O Ethereum continua a evoluir, com atualizações e melhorias constantes que buscam atender às demandas crescentes e manter sua posição como uma plataforma robusta para contratos inteligentes e dApps.

A figura 3.1 representa a interconexão de diferentes máquinas virtuais Ethereum, variantes do Ethereum Virtual Machine. Eles são interconectados para executar contratos inteligentes

e aplicativos descentralizados da rede Ethereum, chamados da mesma forma que a máquina específica de sua execução. Cada um deles é distribuído e conectado em rede, de modo que não haja um servidor centralizado. Isso garante a segurança, descentralização e imutabilidade dos dados através de uma *blockchain*. Dessa forma, mais de uma máquina pode fazer uma transação ao mesmo tempo e todos aprovam a integridade do sistema.

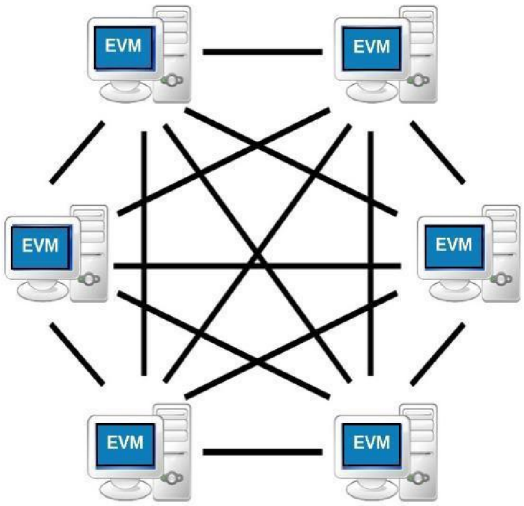


Figura 3.1 – Interconexão entre máquinas executando a Ethereum Virtual Machine (EVM). Fonte: Adaptado de Núcleo do Conhecimento (Nucleo do Conhecimento, 2024).

## 3.2 Arquitetura do Ethereum

A arquitetura do Ethereum foi projetada para ser a base ideal de um sistema de contratos inteligentes e descentralizados e dApps. Para garantir a segurança e a eficácia operacional do sistema, várias camadas colaboram de maneira sinergética. As camadas fundamentais, acumuladas formalmente no protocolo, incluem a camada de execução, consenso e rede. A camada de aplicação, frequentemente referida, é mais uma camada de interface entre o usuário e o desenvolvedor, regulando a interação entre eles por meio de dApps. Todas as quatro camadas são essenciais para a manutenção da rede Ethereum.

### 3.2.1 Camada de Execução

A Ethereum Virtual Machine (EVM) é, sem dúvida, a principal razão para a capacidade de execução no Ethereum. A Máquina Virtual Ethereum é um ambiente de execução geral baseado em pilha, no qual os nós têm a função de executar contratos na rede Ethereum. Esta é uma plataforma que permite a criação de contratos individuais. Basicamente, um contrato é uma função de código fundamentada em Ethereum que pode ser direcionada e implementada pela rede Ethereum. A consistência é garantida pois todos os nós na rede executam o mesmo código da EVM, assegurando que todas as execuções da EVM gerem o mesmo resultado para uma entrada

idêntica. A uniformidade assegura a integridade e a confiabilidade, já que a variação do resultado poderia prejudicar a uniformidade da rede (WOOD, 2014).

Tudo isso pode ser realizado através do uso de uma estrutura de dados para armazenamento de estado conhecida como Trie Merkle Patricia. Em termos técnicos, as Árvores de Merkle e Patricia Tries são uma fusão, possibilitando consultas ágeis e atualizações de estado. Recentemente, as atualizações do Ethereum 2.0 tornaram isso mais eficaz, particularmente no que diz respeito à serialização de dados, utilizando a Serialização Simplificada (SSZ) (FOUNDATION, 2023).

Em relação à integridade dos dados nas Árvores de Merkle, é geralmente garantida usando uma *hash tree*. Cada folha da Árvore de Merkle é, portanto, a representação do *hash* de um bloco de dados; e cada nó interno é a representação do *hash* dos filhos. Portanto, o usuário pode verificar a integridade de uma forma muito eficaz e segura. Por outro lado, existem árvores otimizadas chamadas Patricia Tries, que são usadas para armazenar dados associativos, permitindo recuperações e atualizações rápidas. Patricia Trie é uma organização de dados eficiente que suporta operações rápidas de inserção e busca.

A EVM pode verificar de forma eficaz e rápida o estado do *blockchain* por meio das estruturas combinadas em uma Merkle Patricia Trie. A qualidade da integridade dos dados é adicionada pela Merkle Trie através de *hashing*; as vantagens das operações de busca e atualização de maneira eficiente são trazidas pela Patricia Trie. Em ordem adequada, essa configuração híbrida está bem posicionada para validar transações e blocos de alta velocidade, sendo, portanto, necessária para o funcionamento essencial da rede Ethereum (WOOD, 2014).

Ela gerencia e atualiza o estado do *blockchain*, processa transações e cria novos blocos de forma que possa empregar contratos inteligentes que possam interoperar com outros contratos e estados do *blockchain*. Oferece operações muito amplas e processos bastante complexos (WOOD, 2014).

A figura 3.2.2 demonstra o fluxo de compilação de um código escrito em Solidity até sua execução na Ethereum Virtual Machine (EVM). O código Solidity é inicialmente compilado, gerando o *bytecode* da EVM, que é, então, executado na EVM. A Ethereum Virtual Machine processa as transações e atualiza o estado do *blockchain*, permitindo a implantação de contratos inteligentes que podem interagir com outros contratos e estados na rede. Esse processo é essencial para garantir a integridade e a descentralização da rede Ethereum.

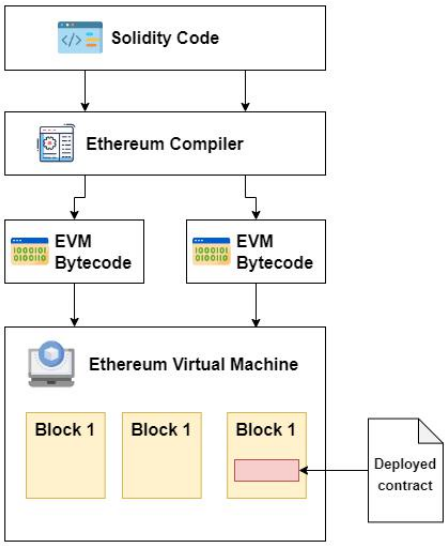


Figura 3.2 – Fluxo de compilação do código Solidity até a implantação no Ethereum Virtual Machine. Fonte: Adaptado de Metlabs (Metlabs, 2024).

### 3.2.2 Camada de Consenso

No protocolo Ethereum, a camada de consenso requer que todos os nós mantenham-se atualizados sobre o avanço da rede de blocos. No começo, o Ethereum utilizava uma camada de consenso fundamentada na prova de trabalho, um procedimento bastante parecido com o utilizado pelo Bitcoin. Neste modelo, os mineiros disputavam para resolver problemas computacionais complexos e obtinham prêmios pela inclusão de novos blocos na *blockchain*. O lançamento da versão 2.0 do Ethereum modificou tudo isso, redirecionando o mecanismo de consenso para a *proof of stake* (BUTERIN et al., 2014).

A principal distinção entre PoW e PoS reside na abordagem dada à segurança e validação. Sem o PoW, a proteção da rede estaria sujeita à competição de computadores. Os mineradores alocam uma vasta energia e capacidade de processamento para solucionar algoritmos complexos e inserir as transações nos blocos. Em um procedimento que requer tanta capacidade de processamento, a utilização de energia também é elevada, levando a um consumo considerável de eletricidade e provocando impactos ambientais consideráveis (KIAYIAS et al., 2017).

Em contrapartida, o PoS emprega um processo distinto que valida as transações com base no número de tokens apostados pelos validadores. No *proof of stake*, a seleção dos validadores para a construção de novos blocos é baseada na quantidade de Ether que eles possuem e estão dispostos a 'apostar' como garantia. Isso diminui consideravelmente o uso de energia, já que os cálculos não são tão intrincados e demandantes. A segurança é fundamentada na integridade dos verificadores e na importância que eles representam para o sistema (BUTERIN et al., 2014).

Além de ser mais eficaz no uso de energia, o PoS oferece um desempenho superior na rede, principalmente por não haver a mesma competição presente no PoW. No PoS, as condições

de validação não provocam tanta competição quanto no PoW, levando a tempos de bloqueio mais ágeis e uma capacidade de processamento de transações mais elevada. Isso o faz mais expansível e com uma latência reduzida na rede (BUTERIN et al., 2014). Portanto, a estrutura do PoS proporciona uma maior resistência a ataques, já que um atacante precisaria de um grande volume de Ether para danificar a rede, o que é economicamente impraticável.

A camada de consenso abrange também a Beacon Chain, o núcleo do Ethereum 2.0, responsável por coordenar o consenso entre diversos *shards* e validadores. A Beacon Chain visa organizar a comunicação entre os *shards* e assegurar a sincronização de todos os elementos da rede (BUTERIN et al., 2014).

A figura 3.2.2 compara os dois principais mecanismos de consenso implementados em *blockchains*: PoW e PoS. Quanto mais poder computacional um nó participante usa para validar as transações, maior será a sua recompensa. O mecanismo PoS, por sua vez, é baseado em quais e quantas moedas os validadores possuem e "apostam" na rede. Acima destacam-se diferenças importantes entre os dois modelos, incluindo consumo de energia, recompensas e risco de ataque de 51%.

Figura 3.3 – Comparação entre *proof of work* e *proof of stake*. Fonte: Adaptado de SketchBubble (SketchBubble, 2024).

### 3.2.3 Camada de Rede

A camada de rede do Ethereum é encarregada de administrar a comunicação entre os nós que formam a rede - uma análise representativa não poderia incluir esse elemento crucial da operação distribuída e descentralizada do Ethereum. No Ethereum 1.0, o protocolo DevP2P regula a comunicação entre nós, definindo como os nós se localizam, criam uma conexão e

como os dados são transmitidos. DevP2P é um protocolo utilizado para comunicação direta e intercâmbio de informações na rede Ethereum.

Com a introdução do Ethereum 2.0, o LibP2P foi adotado em vez do DevP2P. LibP2P é uma biblioteca modular que possibilita uma estrutura de comunicação mais adaptativa e expansível entre os nós. Ela promove a união de diversos módulos de comunicação e identificação de pares, visando tornar a rede expansível e segura. O LibP2P oferece recursos avançados, como a identificação de pares e a comunicação criptografada, essenciais em uma rede shardizada para o funcionamento eficaz da rede (TEAM, 2019).

### 3.2.4 Camada de Aplicação

Na *blockchain*, a camada de aplicação é encarregada de criar e executar contratos inteligentes e aplicativos descentralizados dApps (GARROCHO, 2022).

Um contrato inteligente, é um programa independente que corre na *blockchain* (por exemplo Ethereum), automatiza processos e transações sem intermediários como bancos ou plataformas centrais. Estes contratos podem ser usados para fazer automaticamente transferência de fundos, por exemplo, ou validar acordos entre duas partes. A linguagem mais popular para codificar esses contratos é Solidity, que é projetada especialmente para a *blockchain* Ethereum (TYAGI et al., 2023).

Juntamente aos contratos inteligentes, os aplicativos descentralizados compõem a segunda camada, apresentando segurança e capacidade de verificação de operações em uma relação de igual para igual. São usados em serviços financeiros (da área de empréstimo), jogos onde os ativos estão no *blockchain* principal sob controle do usuário e até em mesmo redes sociais. A camada possibilita que ações sejam realizadas pelos usuários de forma direta, sem intermediários, como nas transações. Na aplicação financeira descentralizada DeFi, é possível que duas pessoas emprestem e peguem dinheiro emprestado uma da outra, sem qualquer intermediação de bancos ou qualquer outra instituição financeira, com base nas condições estabelecidas por contrato inteligente. Portanto, a camada de aplicação é crucial na criação de soluções descentralizadas que permitem contratos inteligentes e *dApps* transformarem indústrias e melhorarem a segurança e automação na *blockchain* (GARROCHO, 2022).

## 3.3 Geth (Go-Ethereum)

### 3.3.1 O que é o Geth?

Geth, ou Go-Ethereum(Ethereum Foundation, 2015), é uma variante popular do protocolo Ethereum, desenvolvida na linguagem de programação Go. O Geth, criado e gerenciado pela Fundação Ethereum, é crucial para o funcionamento e a manutenção da *blockchain* Ethereum. Desde

a sua implementação, Geth tem se destacado como uma das implementações mais empregadas e usadas, proporcionando uma solução sólida e eficaz para se conectar à rede Ethereum.

O Geth, atuando como um cliente Ethereum, possibilita que usuários e programadores se conectem à rede Ethereum, participando da validação de transações e blocos. O Geth, com sua poderosa interface de linha de comando, possibilita uma vasta variedade de operações, como a realização de contratos inteligentes e a extração de blocos. Esta interface é fundamental para programadores que precisam de instrumentos para depuração e interação direta com a rede.

O Geth pode ser ajustado de diversas formas para satisfazer as demandas e capacidades do usuário. No modo completo, o Geth baixa e verifica toda a cadeia de blocos desde o começo, assegurando que cada transação e bloco seja verificado localmente. Este método é crucial para aqueles que desejam contribuir para a proteção da rede e examinar de maneira autônoma a situação da *blockchain*. Em contrapartida, o modo leve possibilita que o Geth funcione sem a exigência de armazenar toda a *blockchain*, mas apenas uma parte dos dados necessários para sua operação. Este modo é apropriado para aparelhos com funcionalidades restritas ou para usuários que procuram uma sincronização mais ágil com a internet. O método de arquivo permite acessar e examinar o estado integral da *blockchain*, sendo especialmente benéfico para pesquisadores e analistas que precisam de uma perspectiva completa da rede. Cada forma de funcionamento impacta a forma como o Geth se relaciona com a rede e o tipo de informações que guarda, impactando a eficácia e a segurança das operações executadas (FOUNDATION, 2024).

### 3.3.2 Clientes Ethereum

#### 3.3.2.1 Clientes de Execução

Clientes operacionais, como o Geth, desempenham o papel de administrar a Máquina Virtual Ethereum (EVM), vital para a infraestrutura do Ethereum. A EVM possibilita a execução de contratos inteligentes e operações na rede, mantendo uma cópia completa da *blockchain* que executa os contratos conforme as instruções dos programadores.

A EVM age como um ambiente de execução isolado e determinístico, garantindo que todas as suas instâncias produzam os mesmos resultados ao executar o mesmo contrato inteligente. Esta propriedade é vital para a consistência da *blockchain* e para a confirmação segura das transações. A EVM emprega uma estrutura conhecida como Merkle Patricia Trie para administrar o estado da *blockchain*, que une os benefícios das Merkle Trees e das Patricia Tries. Isso possibilita que Geth e outros clientes efetuem verificações rápidas e acuradas do estado atual da *blockchain*, além de validarem transações e blocos (UCBAS et al., 2023).

Adicionalmente, os clientes que executam supervisionam e atualizam a *blockchain*, realizam operações e originam blocos. Eles usam algoritmos de consenso, como o modelo de *proof of work* ou *proof of stake*, projetados para garantir a segurança e a natureza inviolável de uma *blockchain*. A eficácia e segurança da rede dependem seriamente da capacidade dos usuários de

processar e validar transações de forma eficiente e segura.

#### 3.3.2.2 Clientes de Consenso

Apesar dessa transformação significativa na estrutura da rede, provocada pela transição para o Ethereum 2.0, é a implementação de um mecanismo de *proof of stake* em vez de *proof of work* que terá um papel crucial no novo contexto. A principal tarefa de manter a rede em termos de integridade e segurança agora será dos clientes de consenso.

Clientes de consenso são responsáveis pela validação de blocos e pela coordenação entre os validadores. No modelo PoS, os validadores são escolhidos proporcionalmente à quantidade de Ether que possuem e estão dispostos a 'apostar' como garantia. Esse sistema pode criar um incentivo para um comportamento honesto, pois um validador malicioso perderá parte de sua participação. Os clientes de consenso conectam os validadores com a Beacon Chain, ajudando a coordenar a criação e validação de novos blocos. Eles garantem que todas as partes de uma rede concordem sobre o estado atual da *blockchain* (LABS, 2021).

Isso é uma parte crítica para a operação eficaz e segura do Ethereum 2.0. Eles garantem que os nós estejam de acordo com o estado da *blockchain*, e que a adição de blocos seja sempre feita de maneira consistente e segura. A combinação de clientes de consenso e de execução é, portanto, um componente indispensável para o correto funcionamento da rede Ethereum, pois valida e executa transações adequadas que processam contratos inteligentes (LABS, 2021)."

### 3.3.3 Beacon Client

Beacon Client é um componente central da 2,0 Ethereum, encarregada de cuidar da Beacon Chain, que coordena a atividade dos validadores e *shards* ligados na rede. A Beacon Chain é o ponto central do novo mecanismo de consenso *proof of stake* (PoS) e desempenha um papel crucial na sincronização e validação de blocos em uma rede *shard*.

O Beacon Client simplifica a interação entre *shards* e auxilia os validadores na organização de suas tarefas. Gerencia a distribuição de recompensas e sanções, visando estimular os validadores a agir de forma justa e garantir a segurança da rede. A Beacon Chain não só organiza a concordância entre os variados *shards*, como também garante que todos os elementos da rede estejam sincronizados e cooperem mutuamente.

A implementação do Beacon Chain é um progresso notável em comparação ao modelo anterior de consenso PoW, proporcionando um método mais expansível e eficaz para validar e coordenar na rede Ethereum. O Beacon Client permite o funcionamento eficiente do novo sistema PoS, coordenando as ações dos validadores e a formação de blocos em um ambiente *shardizado*.

## 3.4 Aspectos Técnicos

### 3.4.1 Networking

#### 3.4.1.1 Estrutura de Rede P2P

A rede Ethereum é arquitetada no paradigma P2P (*peer-to-peer*), com todos os pares conectados diretamente uns aos outros por meio da rede. A arquitetura P2P, descentraliza e simplifica o sistema, no qual cada par é igual a qualquer outro par na rede. Todas as comunicações são diretas; desta maneira, não há um servidor central que possa conduzir a operação realizada na rede. A rede Ethereum é, portanto, descentralizada entre seus pares, com cada par possuindo e participando da transação e validação de blocos. A natureza P2P é vital para a segurança e robustez da rede.

A descentralização da rede P2P impede que ocorram falhas ou ataques coletivos. Como ocorre a descentralização, nenhuma parte estaria no controle da rede e, portanto, resistiria a potenciais correntes de ataque ou falha. Adicionalmente, a operação de emparelhamento entre os pares é o que impulsiona a eficácia da arquitetura P2P. Cada transação é propagada entre os pares de forma rápida e sem obstruções (FOUNDATION, 2024).

A figura 3.4.1.1 compara duas arquiteturas de rede: cliente-servidor e P2P. O primeiro descreve um servidor centralizado que organiza a coordenação e a comunicação com os clientes. O segundo apresenta nós que se comunicam diretamente entre si e não dependem de um servidor central. Isso permite evitar situações em que pontos únicos de falha afetam a rede inteira e distribuem a carga entre os nós. A rede Ethereum é baseada em uma arquitetura P2P, já que vários grupos de nós têm especializações diferentes, permitindo que todos pares participem da validação e da propagação das transações.

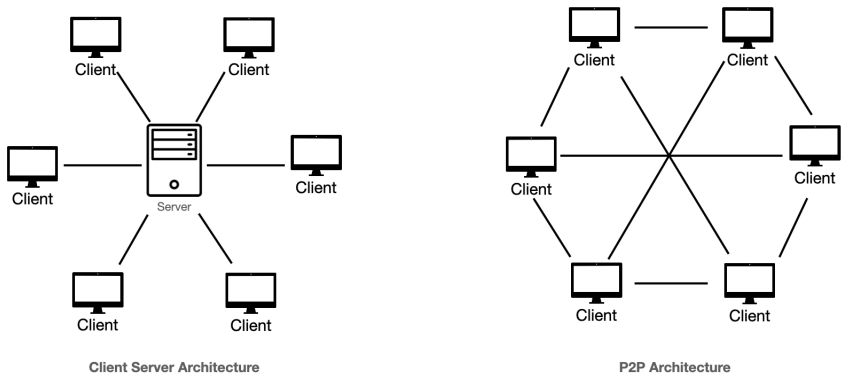


Figura 3.4 – Comparação entre arquitetura cliente-servidor e arquitetura P2P. Fonte: Adaptado de Medium (Nilay Güler, 2024).

#### 3.4.1.2 Comunicação através de Protocolos

Em Ethereum 1.0, a comunicação entre os nós era gerenciada por DevP2P, um protocolo que inclui vários sub-protocolos para diferentes tipos de dados da rede, como blocos, transações e dados de estado. Esse protocolo é responsável pela troca de mensagens e descoberta de pares, garantindo que cada nó possa encontrar e se comunicar com outros na rede (FOUNDATION, 2024).

A comunicação por meio de protocolos foi adaptada em Ethereum 2.0. Em vez de DevP2P, foi adotado o LibP2P como o protocolo responsável. LibP2P é uma biblioteca modular, desenvolvida com uma abordagem mais flexível do que seus antecessores, que oferece submódulos prontos para uso, como descoberta de pares, criptografia de comunicações de rede e transporte de dados criptografados (TEAM, 2019). Essa abordagem flexível reflete um contexto em que o protocolo anterior já não conseguia acompanhar as novas capacidades de rede exigidas, como a necessidade de uma rede em *shard* e maior segurança e escalabilidade.

### 3.4.2 Peer Discovery & Management

#### 3.4.2.1 Resistência a Ataques Sybil na Rede Ethereum

A resistência a ataques Sybil é um dos pilares cruciais que visam tornar a rede Ethereum segura. Um ataque Sybil ocorre quando um ator mal-intencionado tenta comprometer o funcionamento da rede mediante a criação de várias identidades falsas para ganhar controle majoritário e influenciar a validação de blocos ou transações de maneira desonesta. Tal ameaça se mostra altamente possivelmente para redes descentralizadas, nas quais reina a confiança e onde o consenso entre os participantes é vital (PLATT; MCBURNEY, 2023).

No entanto, o Ethereum mitigou tais riscos com mecanismos robustos. Em primeiro lugar, no Ethereum 2.0, o *proof of stake* é uma defesa eficaz contra os ataques Sybil. Visto que é necessário comprometer uma quantidade significativa de Ether para ser um validador na rede, a criação de múltiplas identidades virtuais se torna consideravelmente difícil e impossível de ser economicamente rentável para uma entidade mal-intencionada (ORLICKI, 2020). Pode certamente ser feito, mas, quanto mais identidades, mais investimento, o que dissuade o crime.

Em segundo lugar, o Ethereum implementa um rígido sistema de validação e punição. As validações incorretas são detectadas, bem como comportamentos fraudulentos ou maliciosos em tentativas de ataque à rede, o que leva à punição dos validadores maliciosos por meio do *slash* (BHUDIA et al., 2023). Assim, a seleção de validadores é feita com atenção, enquanto os s*lashing* separados garantem que os validadores ajam corretamente, promovendo a segurança da rede.

Além disso, a resistência a ataques Sybil e criptoeconômicos contribuem para alta disponibilidade. Eles são responsáveis por manter o sistema funcionando, mesmo em caso de tentativas de controle ou fraude, levando a um ecossistema mais confiável. Isso ocorre porque o Ethereum

atua como fornecedor de um serviço resistente a falhas, diminuindo assim o impacto de um ataque. A finalidade aqui é assegurar segurança para a continuação do funcionamento da rede e ativos digitais, permitindo transações ininterruptas e troca (PAVLOFF; AMOUSSOU-GUENOU; TUCCI-PIERGIOVANNI, 2022).

#### 3.4.2.2 Prevenção de DoS

A prevenção de ataques de negação de serviço é crítico para manter a integridade e a eficiência da rede Ethereum. Os doS atacam saturando a rede com pedidos inválidos e maliciosos que a incapacitam de operar de forma eficiente. Para prevenir o doS, é possível implementar mecanismos que incluam limites de taxa, verificações de consumo de recursos e filtra ativos do mecanismo de filtragem de pacotes. O Ethereum implementa limites na largura de banda e na capacidade de processamento de cada nó, e, com a atualização para Ethereum 2.0, o protocolo de consenso *proof of stake* contribui para a resistência DoS mais robusta (AUMASSON; KOLEGOV; STATHOPOULOU, 2021). Além disso, a filtragem e a rejeição de transações e blocos suspeitos são melhoradas, o que mantém a integridade da rede e impede que ela seja atacada pela sobrecarga. Independentemente das ameaças, as melhorias no protocolo e na arquitetura garantem a operação ininterrupta da rede (GREENE; JOHNSTONE, 2018).

#### 3.4.2.3 Pontuação de Nós na Rede Ethereum

A pontuação do peers é uma parte fundamental da avaliação da qualidade e da confiabilidade dos operadores no Ethereum. (FOUNDATION, 2024) esclarece que a pontuação do peers é baseada no desempenho da maioria e na confiabilidade e positividade dos pares. No Ethereum 2.0, a pontuação e a seleção de nós são incorporadas ao protocolo PoS; portanto, os pares com melhor desempenho terão maior probabilidade de serem utilizados na validação de transações e blocos. Este método incentiva os operadores a ter uma boa classificação e uma forte contribuição para a rede, fato que promove a segurança da rede e sua robustez. Dessa forma, a rede Ethereum permanece estável e eficiente na operação cotidiana (ZHANG; LI; DUAN, 2024).

#### 3.4.2.4 Propagação de Dados na Rede Ethereum

O mecanismo de *gossip* permanece sendo uma técnica primária para a propagação de blocos e transações sobre a rede Ethereum. O (PEASE; SHOSTAK; LAMPORT, 1980) descrevem o mecanismo de *gossip* como a capacidade de cada nó a transmitir pequenas quantidades de informações para um grupo de pares conhecidos, o qual, por sua vez, vai retransmitir essa informação para outros nós. É assim que a informação corre pelos nós e garante que não é necessário que cada nó comunique com todos os outros nós diretamente. Deste ponto de vista, a propagação de dados pode ser entendida como um tipo de comunicação estigmérgica. Como num sistema biológico, a propagação estigmérgica assenta na comunicação indireta entre os próprios nós da rede, em que as ações de um nó afetam o ambiente – o que afeta, por sua vez, a forma

como os restantes nós vão reagir. Assim, não é necessária uma entidade central que determine a forma como os blocos e transações se propagam, uma vez que é o ambiente que determina a forma como os primeiros formam segundo respondendo a um ambiente que foi moldado pelas informações que correm entre os nós. Essa abordagem garante que a rede Ethereum consegue distribuir blocos e transações eficientemente – sem gastar demasiada largura de banda e com latências relativamente pequenas, especialmente tendo em conta os ganhos alcançados com a afinação do Ethereum 2.0.

#### 3.4.2.5 Rastreamento da Árvore de Blocos

A *blockchain* do Ethereum é estruturada como uma cadeia de blocos, onde cada bloco referencia um bloco anterior, formando uma sequência contínua e imutável de blocos. (NAKAMOTO, 2008) fornece uma base para entender a estrutura e a segurança da cadeia de blocos, destacando que cada bloco contém um *hash* do bloco anterior, garantindo a integridade e a continuidade da cadeia. O rastreamento da árvore de blocos é crucial para garantir que a *blockchain* permaneça consistente e segura. Cada bloco na cadeia contém um *hash* que referencia o bloco anterior, criando uma sequência imutável e verificável de blocos. Essa estrutura assegura que qualquer tentativa de alterar um bloco seja detectada, pois alteraria todos os *hashes* subsequentes, invalidando a cadeia. Com a introdução da Beacon Chain no Ethereum 2.0, a sincronização e o rastreamento da *blockchain* foram aprimorados, contribuindo para a escalabilidade e segurança da rede (NAKAMOTO, 2008).

#### 3.4.2.6 Reorganizações de Blockchain e Resolução de Forks

Reorganizações de *blockchain*, ou *re-orgs*, ocorrem quando há uma mudança na cadeia principal devido a *forks* ou blocos concorrentes. (DECKER; WATTENHOFER, 2013) discutem como redes *blockchain*, como o Bitcoin, lidam com reorganizações e *forks*. De maneira similar, a rede Ethereum adota o princípio de selecionar a cadeia mais longa e válida para garantir a integridade da *blockchain*. Com uma reorganização, a rede seleciona a cadela mais longa e a adota como a principal, despejando blocos da cadeia mais curta.

Isso é crítico para manter a *blockchain* como um todo e todos ecologicamente corretos, porque elimina a incerteza e garante que todos os nós de uma rede estejam alinhados com uma versão da cadeia. Agora, com o Ethereum 2.0 e o mecanismo de consenso *proof-of-stake*, a abordagem para *re-orgs* e também *forks* foi alterada, o que implica que, embora existam *re-orgs* e *forks*, a *blockchain* está funcionando seguramente. A gestão de *re-orgs* é vital para resolver conflitos e garantir que a *blockchain* continue a operar de forma saudável e segura, independentemente de *forks* ou emendas.

#### 3.4.2.7 Mempool de Transações no Ethereum

O *mempool* é um elemento central da arquitetura do Ethereum. Este é um depósito de transações em espera, enquanto elas ainda não foram incluídas nos blocos. Segundo (MILLER et al., 2016), o *mempool* possibilita que os mineradores, ou validadores no caso do mecanismo de *proof-of-stake*, estabeleçam a ordem de prioridade das transações com base nas taxas de gas disponíveis. Em outras palavras, as transações que envolvem taxas de gas mais elevadas serão inicialmente processadas, pois proporcionam uma maior compensação financeira para o validador. Assim, optar por requisitar uma taxa de gas menor fará com que a transação demore mais a ser processada.

A variação das taxas de gas também depende do nível de congestionamento da rede. Quando a demanda por processamento de transações é alta, as taxas aumentam, o que influencia diretamente o tempo de processamento das transações. Assim, o *mempool* se adapta a essas condições de congestionamento, permitindo uma priorização dinâmica.

Com a introdução do EIP-1559, o mecanismo de taxas de gas no Ethereum foi reformulado, estabelecendo uma taxa base e uma gorjeta (*tip*) opcional. A taxa base é queimada, reduzindo a oferta total de ETH, enquanto a gorjeta é direcionada aos validadores como incentivo para incluir transações. Essa mudança afeta ainda mais a dinâmica de como as transações são priorizadas no *mempool*, oferecendo uma abordagem mais eficiente e previsível para a inclusão de transações nos blocos.

Os nós também validam as transações antes de inseri-las no *mempool*, para que apenas transações válidas possam ser escolhidas para inclusão nos blocos subsequentes, garantindo a integridade da rede. Somente transações que seguem as regras da *blockchain* podem ser processadas. Essas funções centrais para a operação da rede permanecem após a transição do PoW para o PoS, onde validadores, em vez de mineradores, escolhem as transações, mas o *mempool* e a lógica de seleção com base nas taxas de gas ainda são mantidos. No caso do Ethereum 2.0, por exemplo, conforme mencionado (MILLER et al., 2016), o processo continua semelhante, com mudanças na maneira como os validadores priorizam as transações.

A figura 3.4.2.7 apresenta o processo de *mempool* no Ethereum, onde as transações aguardam para serem incluídas em blocos. As transações com taxas de gas mais elevadas são priorizadas pelos mineradores ou validadores, maximizando seus ganhos. A priorização de transações é crucial para o Ethereum, por permitir que as transações mais lucrativas sejam processadas primeiro. Consequentemente, as transações com taxas menores podem levar mais tempo para serem confirmadas, especialmente durante períodos de alta demanda na rede. O EIP-1559 reformulou o modelo de taxas no Ethereum. Ele introduziu uma taxa base que é queimada mais uma gorjeta opcional para incentivadores.

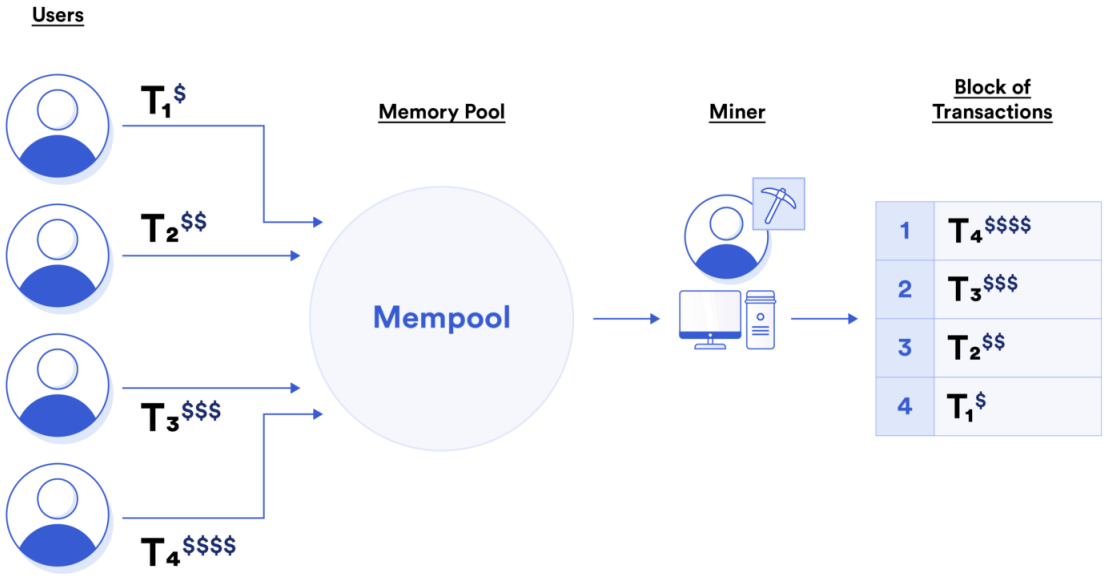


Figura 3.5 – Funcionamento do Mempool e priorização de transações no Ethereum. Fonte: Adaptado de Hub do Investidor (Hub do Investidor, 2024).

#### 3.4.2.8 Sincronização

A sincronização entre os nós da rede Ethereum garante que todos os nós tenham uma visão ou estado da *blockchain*. De acordo com (BUTERIN et al., 2014). A sincronização completa faz o *download* e a verificação de todos os blocos da cadeia inteira, começando do bloco gênese, para que o nó tenha uma cópia completa da *blockchain*. Isso permite que os nós possam obter o estado atual da *blockchain* eficientemente, baixando somente os novos blocos, juntamente com os dados de estado.

A introdução da Beacon Chain no Ethereum 2.0 com novos mecanismos de sincronização otimizou a coordenação entre os validadores. A Beacon Chain simplifica a organização do consenso entre os validadores e traz mecanismos que aumentam a eficácia dos processos de sincronização, para que novos nós sejam assimilados na rede muito mais rapidamente. Também permite uma sincronização rápida sempre que novos nós se juntam a uma rede, baixando seletivamente apenas os blocos recentes e alguns dados críticos, permitindo que esses nós participem facilmente da validação das transações. Isso reduz a latência e, consequentemente, a vulnerabilidade a ataques como o gasto duplo, com o tempo para a finalização dos blocos minimizado, algo que, de fato, aumenta a segurança da rede.

Nesse sentido, essas melhorias na sincronização tornam a rede Ethereum ainda mais escalável e segura, permitindo que continue crescendo de forma descentralizada e eficiente. Isso reforça que a sincronização rápida e eficiente é indispensável para manter a natureza descentra-

lizada do Ethereum, com a coordenação das atividades pelos validadores ocorrendo de forma distribuída e segura, o que melhora a segurança e a integridade geral do *distributed ledger*.

## 3.5 Comparação das Tecnologias do Ethereum

### 3.5.1 Introdução

A transição do Ethereum 1.0 para o Ethereum 2.0 no Ethereum inclui alterações significativas nas tecnologias subjacentes. Em outras palavras, era necessário atualizar o sistema, uma vez que a rede existente não era escalável e segura.

Esta seção fornecerá uma visão geral das principais tecnologias, inovações e melhorias envolvidas. Essas áreas incluem abordagens de comunicação em redes ponto a ponto, como LibP2P em execução com Ethereum 2.0, pois distribui a rede de comunicação em comparação com abordagem DevP2P na versão anterior. A descoberta de pares avançou de Discv4 para Discv5 e a serialização de dados de transação mudou de RLP (*Recursive Lenght Prefix*) para SSZ *(Simple Serialize)*.

Por fim, a abordagem de *hashing* foi alterada de Sha256 para Keccak, a assinatura digital evoluiu de ECDSA (*Elliptic Curve Digital Signature Algorithm)* para BLS (*Boneh-Lynn-Shacham*), o que também foi mencionado no início devido à prioridade de segurança.

A figura 3.5.1 compara a diferença entre os mecanismos de consenso PoW e PoS implementados no Ethereum. No PoW, Ethereum apresenta uma única cadeia monolítica onde a camada de consenso está integrada com a execução. No entanto, após a transição para Ethereum 2.0, o modelo mudou para a divisão em duas camadas: consenso que será chamado de CL e de execução que será chamada de EL. Elas operam através de uma API.

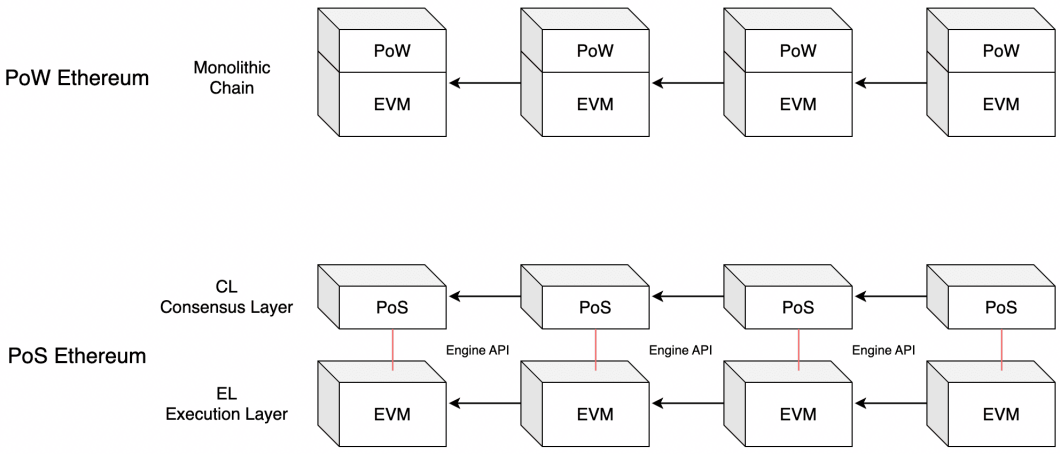


Figura 3.6 – Comparação entre PoW e PoS no Ethereum. Fonte: Adaptado de Luo Zhu (Luo Zhu, 2024).

### 3.5.2 LibP2P

O LibP2P é uma biblioteca modular para redes ponto a ponto, desenvolvida inicialmente para o projeto IPFS (*InterPlanetary File System*) (BENET, 2014) e usada extensivamente no Ethereum 2.0 (WOOD, 2014). Diferente dos protocolos monolíticos, o LibP2P é baseado em módulos, permitindo que diferentes subsistemas de rede sejam misturados e adaptados. Diversos módulos de rede são inclusos, como os de descoberta, transporte, criptografia e multiplexação. A abordagem modular do LibP2P confere flexibilidade ao protocolo, permitindo que cada sistema seja substituído e adaptado separadamente, conforme as necessidades de cada aplicação específica.

Outros algoritmos modernos e eficientes estão no cerne da descoberta de correspondentes na LibP2P. Esses incluem a implementação da Tabela *Hash* Distribuída (DHT) Kademlia, um protocolo eficiente para localizar nós fisicamente mais próximos, que torna o crescimento robusto e escalável de uma rede provável. Além disso, a compatibilidade com o *Domain Name System* converte nomes de servidores de domínio e zonas de autoridade em endereços IP, garantindo maior velocidade na pesquisa e alinhamento com servidores específicos.

O LibP2P tem módulos para proteger a comunicação entre pares contra ataques e interceptações de clientes maliciosos. Ele utiliza RSA *(Rivest-Shamir-Adleman)* para criptografar a conexão entre pares, enquanto o algoritmo simétrico AES *(Advanced Encryption Standard)* é empregado para garantir a máxima privacidade na pós-criptografia.

O LibP2P é uma tecnologia de grande flexibilidade e adaptabilidade de redes, contém elementos essenciais para suportar a criação do Ethereum 2.0 em uma rede *sharded* (WOOD, 2014). No Ethereum 1.0, o *blockchain* sofreu com congestionamentos devido à arquitetura monolítica. Com a introdução do *sharding* no Ethereum 2.0, o LibP2P é fundamental para proporcionar uma troca de dados eficiente entre os *shards*.

Além disso, o conceito de *sharding* facilita a expansão de cada fragmento da rede para processar mais transações das menores partes do bloco, permitindo a execução paralela de várias transações de diferentes fragmentos sem perda de eficiência. Outro fator destacado é a segurança descentralizada da rede, permitindo que ela responda mesmo a ataques distribuídos, inclusive ataques de negação de serviço distribuído, ou DDoS. Se um módulo de *hardware* for comprometido por *hackers*, ele pode ser isolado e substituído sem comprometer a imunidade de todo o sistema.

### 3.5.3 DevP2P

No Ethereum 1.0, o protocolo de interação entre os participantes é denominado DevP2P. Inicialmente, DevP2P foi estabelecido para fornecer os canais de comunicação essenciais para o funcionamento da rede descentralizada do Ethereum 1.0. Assim, naquele período, o DevP2P e sua combinação de protocolos eram a solução mais eficaz para assegurar a integridade e a consistência da *blockchain*. Antes da invenção do LibP2P, o DevP2P foi desenvolvido para criar

uma solução eficaz para a troca de mensagens e a descoberta de *peers* sobre a Ethereum.

O conjunto de protocolos DevP2P opera em uma estrutura hierárquica e inclui vários protocolos de camadas e subprotocolos. O protocolo de descoberta de *peers*, sendo a parte mais importante, permite que os nós encontrem e se conectem entre si quando estiverem conectados à Ethereum. O DevP2P utiliza um sistema de mensagens para informar a todos os outros nós sobre sua existência e mantê-lo simultaneamente por criar uma lista de pares conhecidos. O DevP2P consiste em vários sub protocolos da *blockchain* como sincronização de quadra e sincronização de transação. Esse sub protocolos garantem que todos os outros nós estejam na mesma página que a *blockchain* e fornecem maneiras eficientes de partes transferirem blocos das cadeias uns dos outros e transmitirem transações empacotadas de forma confiável. Outro papel crucial do DevP2P é a comunicação de transações e o compartilhamento de dados de estado, garantindo a integridade e a coesão da *blockchain* ao longo de toda a rede (FOUNDATION, 2024).

Enquanto isso, à medida que a rede Ethereum crescia desde 2015, o DevP2P começava a se mostrar cada vez mais inadequado. Sua falta de modularidade, inadequação para um número crescente de nós e arquitetura fixa começaram a apresentar problemas com a escalabilidade e a manutenção da rede. À medida que o número de transações e nós ativos aumentava, o DevP2P se tornava mais lento. Afinal, não foi concebido para poder dar resposta a um número de transações e um número crescente de nós ativos. Assim, o LibP2P foi desenvolvido como um substituto do DevP2P na progressão da rede Ethereum, conhecida como Ethereum 2.0. Ao contrário de seu antecessor, o novo protocolo é modular e substituível e, portanto, mais adequado para lidar com as crescentes demandas por escalabilidade e flexibilidade. Portanto, este protocolo é mais seguro e adaptável por natureza.

O Discv5 é o protocolo de descoberta de pares que substitui o velho Discv4 em utilização no Ethereum 2.0, otimizando o algoritmo DHT baseado em Kademlia no Ethereum. O Kademlia DHT organiza uma estrutura distribuída que possibilita a localização eficiente de pares em diferentes *shards*. Isso se deve ao fato de muito mais nós estarem sendo utilizados, visto que a rede Ethereum 2.0 é fragmentada em *shards* interconectados que restrigem pares de se comunicarem diretamente. Seu uso em redes com alta fragmentação como o Ethereum 2.0 depende de um protocolo eficiente e ágil para a descoberta de pares (SCHOEDON, 2020).

O Discv5 é inovador por possibilitar a operação em uma rede *shardizada*, constituindo uma forma escalável e resiliente de resolver o problema de descoberta de pares além de utilizar criptografia assimétrica para proteger mensagens, garantindo a autenticidade das informações e prevenindo inúmeras formas de ataques, como *man-in-the-middle*. Isso é significativamente melhor que a criptografia utilizada no Discv4, já que o mesmo não era armazenado de maneira eficaz, tornando a estratégia vulnerável a uma ampla variedade de ataques possíveis.

Discv4, usado no Ethereum 1.0, desempenhou bem seu papel no início, mas enfrentou limitações em termos de escalabilidade e segurança à medida que a rede Ethereum crescia. Com o aumento do número de nós, o Discv4 apresentava latência elevada na descoberta de pares e

vulnerabilidades de segurança, uma vez que as mensagens não eram bem criptografadas. Além disso, o Discv4 era ineficiente em grandes redes e incapaz de lidar com a alta variação no número de nós, resultando em problemas de escalabilidade e aumento da latência de descoberta.

A integração do DNS *(Domain Name System)* ao Discv5 melhora ainda mais a resolução de nomes, tornando a localização de nós específicos na rede mais fácil. O DNS converte nomes de domínio em endereços IP *(Internet Protocol)* e introduzi a descoberta de pares na infraestrutura de rede existente, facilitando a localização de nós, especialmente aqueles não disponíveis imediatamente na tabela DHT.

A transição do Discv4 para o Discv5 reflete a crescente complexidade e demanda da rede Ethereum, à medida que mais nós são adicionados. Com a introdução do Discv5, a rede Ethereum ganha mais eficiência na descoberta de pares e uma proteção mais robusta contra possíveis ataques, consolidando o protocolo como um passo significativo em direção a uma rede mais segura e escalável (SCHOEDON, 2020). A opção pelo Keccak em vez do SHA-256 no Ethereum resulta da busca de um algoritmo para o qual seu funcionamento resultasse em um sentido completo para uma *blockchain* moderna, supersegura, capaz de processar todos os tipos de dados. Ao mesmo tempo, embora o SHA-256 seja frequentemente utilizado na *blockchain* de outras criptomoedas, incluindo o bitcoin. Várias razões garantiram ao Keccak maior segurança e adaptabilidade, fazendo dele o algoritmo de *hash* escolhido para o Ethereum.

### 3.5.4 BLS vs ECDSA

No Ethereum (ETH), as transações sempre foram validadas e protegidas por um algoritmo de assinatura digital que garantia que nenhum intermediário assinasse em nome dos produtores. O ECDSA (*Elliptic Curve Digital Signature Algorithm*) foi adotado como algoritmo padrão pela mistura certa entre segurança e desempenho. Entretanto, com o advento do ETH 2.0, a BLS (*Boneh-Lynn-Shacham*) tornou-se inigualável devido aos seus poderes de infinitamente maior capacidade de agregar assinaturas, permitindo novos patamares de escalabilidade (BONEH; DRIJVERS; NEVEN, 2018).

O ECDSA usava curvas elípticas para gerar pares de chaves privadas e públicas usadas para assinar e validar transações. A principal vantagem do ECDSA foi que ele reduzia o tamanho necessário dos pares de chaves e oferecia segurança de alta eficiência ao mesmo tempo que garantia a validação. No entanto, uma principal desvantagem que vinha com ele era que ele não podia suportar a agregação de assinaturas que faziam. Isso logo foi considerado inadequado para *blockchains* de alto tráfego como o Ethereum, que logo perceberam ser um problema ainda maior, já que todas as assinaturas dadas precisavam ser verificadas, já que isso exigia poder computacional adicional e, no final, resultava em blocos ainda maiores.

Com transição para o Ethereum 2.0, o BLS foi a opção de escolha. BLS significa que vários signatários, todos usando chaves públicas diferentes, podem combinar suas assinaturas em

uma assinatura verdadeira, sendo uma aglomeração única. Isso é particularmente útil no novo mecanismo de consenso PoS, que requer que vários validadores assinem o bloco para validar sua existência. O BLS permite aglomerar essas assinaturas, reduzindo a quantidade de dados necessários para compreendê-las, isso, por sua vez, torna a rede muito mais eficiente e aumenta sua capacidade.

Entretanto, o BLS também apresenta desafios. Embora ofereça vantagens consideráveis em termos de agregação de assinaturas, a verificação dessas assinaturas exige mais recursos computacionais em comparação com o ECDSA. Isso ocorre devido ao uso de emparelhamentos bilineares em curvas elípticas, sendo computacionalmente mais intensivos. Apesar dessa complexidade adicional, a redução no tamanho dos blocos e a melhora no tempo de verificação em cenários com inúmeras assinaturas compensam essas limitações em muitos casos.

O ECDSA, foi usado no Ethereum e em outras *blockchains* por muitos anos e possui amplas bases de auditoria e testes de segurança. Por outro lado, o BLS, embora mais recente, não apresentou problemas no Ethereum 2.0 e demonstra ser promissor, especialmente por atender às demandas de escalabilidade e eficiência do novo esquema de consenso. Portanto, a transição do ECDSA para o BLS reflete uma mudança de prioridades da rede Ethereum. O ECDSA foi vital para garantir a segurança em um ambiente onde as assinaturas individuais eram suficientes, mas o software do BLS é mais adequado às necessidades atuais da rede, os quais são validação eficiente de vários blocos assinados. Em resumo, o BLS mostrou ser superior em escalabilidade e eficiência, características críticas para o funcionamento do Ethereum 2.0 (BONEH; DRIJVERS; NEVEN, 2018).

## 3.6 Introdução ao Cosmos Network

O Cosmos Network é uma plataforma projetada para abordar a escalabilidade, interoperabilidade e usabilidade na criação de *blockchains* descentralizadas. Conhecido como a “Internet das Blockchains”, o Cosmos facilita a comunicação entre diferentes *blockchains*, criando um ecossistema de redes interoperáveis. Diferente de outras plataformas, como o Ethereum, que se concentram em uma única cadeia, o Cosmos permite que desenvolvedores criem *blockchains* independentes que podem se comunicar usando o protocolo *Inter-Blockchain Communication* (IBC).

O principal objetivo do Cosmos é resolver as limitações de *blockchains* tradicionais, como dificuldade de escalabilidade, baixa performance e interoperabilidade limitada. Ele atinge isso com uma abordagem modular, permitindo que os desenvolvedores aproveitem o Cosmos SDK (*Software Development Kit*) para criar *blockchains* customizadas, que utilizam o Tendermint Core como motor de consenso.

### 3.6.1 Arquitetura do Cosmos

A arquitetura do Cosmos é projetada para oferecer uma solução modular, interoperável e escalável para a construção de *blockchains* específicas. Ela é composta por três componentes fundamentais que atuam integradamente: o Cosmos SDK, o Tendermint Core e o protocolo Inter-Blockchain Communication (IBC). Esses elementos trabalham juntos para fornecer um ambiente flexível, capaz de atender a diversas demandas da indústria, permitindo a criação de *blockchains* independentes que interagem de maneira harmoniosa no ecossistema.

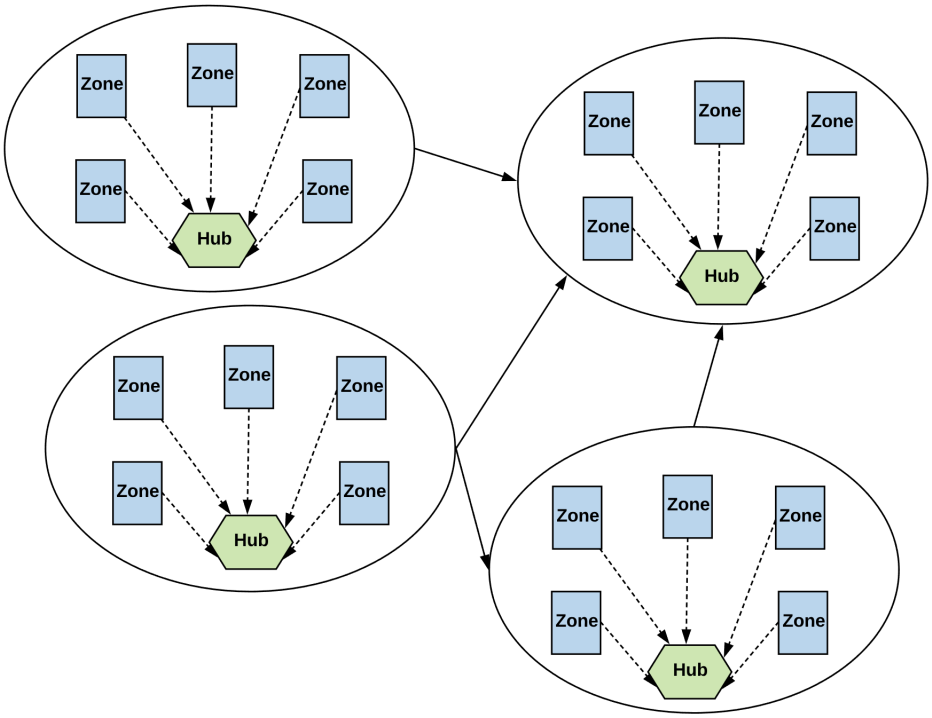


Figura 3.7 – Arquitetura distribuída em múltiplos hubs e zonas no Cosmos Network. Fonte: Adaptado de Preethi Kasireddy (KASIREDDY, 2020).

#### 3.6.1.1 Cosmos SDK

O Cosmos SDK é o núcleo de desenvolvimento da plataforma. Ele foi projetado para simplificar o processo de criação de *blockchains*, oferecendo um *framework* modular que permite construir redes específicas para diferentes aplicações. A principal característica do SDK é sua capacidade de abstrair a complexidade da infraestrutura subjacente, fornecendo bibliotecas e módulos reutilizáveis que implementam funcionalidades essenciais, como transferências de tokens, autenticação e mecanismos de governança (KWON; BUCHMAN, 2018).

O design do Cosmos SDK é baseado na filosofia de "orientação a aplicativos", onde cada *blockchain* é construída como uma aplicação independente, em vez de contratos inteligentes genéricos, como ocorre no Ethereum. Essa abordagem permite que os desenvolvedores se concentrem nas funcionalidades específicas de suas *blockchains*, sem se preocupar com detalhes

de baixo nível (KWON, 2014). A modularidade do SDK é outro ponto crucial. Ele permite que os desenvolvedores personalizem e combinem diferentes módulos, ou mesmo criem novos, para atender às necessidades específicas de cada projeto. Por exemplo, é possível configurar um módulo de staking adaptado para aplicações financeiras ou um módulo de governança voltado para sistemas de decisão coletiva em indústrias.

Além disso, o Cosmos SDK utiliza a linguagem de programação Go, conhecida por sua eficiência e simplicidade, facilitando a criação de aplicações robustas e escaláveis. A segurança também é um pilar fundamental do SDK, com mecanismos para mitigar vulnerabilidades comuns em sistemas descentralizados. Isso o torna uma escolha confiável para aplicações críticas, como sistemas bancários descentralizados e redes industriais de alta complexidade (AMOUSSOU-GUENOU et al., 2018).

#### 3.6.1.2 Tendermint Core

O Tendermint Core é o motor de consenso subjacente que alimenta as *blockchains* criadas com o Cosmos SDK. Ele desempenha um papel central ao garantir a segurança, a ordem e a integridade das transações em uma *blockchain*. Baseado em um modelo de consenso Bizantino (BFT), o Tendermint oferece tolerância a falhas bizantinas, o que significa que a rede pode continuar funcionando mesmo que até um terço dos validadores sejam maliciosos ou falhem (AMOUSSOU-GUENOU et al., 2018).

Uma das principais inovações do Tendermint é seu uso do algoritmo *Proof of Stake*, que elimina a necessidade de mineração intensiva em recursos, característica do *Proof of Work* utilizado em redes como o Ethereum. No PoS, os validadores são selecionados com base na quantidade de tokens que possuem e apostam na rede. Esse modelo não somente reduz o consumo de energia, mas também melhora significativamente a latência e o throughput da rede. Transações são confirmadas de forma quase instantânea, garantindo finalização rápida e eliminando a possibilidade de reorganizações de cadeia, comuns em sistemas baseados em PoW (BELTRANDO; POTOP-BUTUCARU; ALFARO, 2022).

Além de sua eficiência, o Tendermint é altamente adaptável. Ele é projetado para ser agnóstico à aplicação, permitindo que qualquer tipo de *blockchain* seja construída sobre ele. Isso o torna ideal para aplicações industriais que exigem flexibilidade e desempenho, como redes de IoT e sistemas de rastreamento logístico. Outro aspecto importante é a facilidade de integração com sistemas existentes, graças à sua compatibilidade com protocolos padronizados, como o gRPC e o REST.

#### 3.6.1.3 Inter-Blockchain Communication (IBC)

O protocolo Inter-Blockchain Communication (IBC) é o elemento que habilita a interoperabilidade entre as *blockchains* do ecossistema Cosmos. Ele foi projetado para permitir que diferentes redes troquem informações de forma segura e eficiente, sem a necessidade de interme-

diários. Esse protocolo é um dos pilares da visão do Cosmos de uma “Internet das Blockchains”, possibilitando uma comunicação fluida entre redes independentes (GOES, 2020).

O funcionamento do IBC baseia-se em clientes leves e canais de comunicação. Cada *blockchain* envolvida em uma comunicação mantém um cliente leve da outra, que atua como um mecanismo de validação das mensagens recebidas. Isso garante que as transações sejam verificadas de maneira confiável, sem comprometer a segurança. Os canais, por sua vez, são estabelecidos entre as *blockchains* para facilitar o fluxo de informações. Cada canal é isolado, evitando que falhas ou vulnerabilidades em uma conexão afetem outras redes (ESSAID; KIM; JU, 2023).

O IBC permite uma ampla gama de aplicações práticas, como transferências de tokens entre diferentes *blockchains*, sincronização de dados entre redes industriais e execução de contratos em *blockchains* separadas. Um exemplo é a integração de uma *blockchain* para rastreamento de suprimentos com outra para gestão financeira, permitindo que informações de inventário e pagamentos sejam sincronizadas automaticamente. Esse nível de interoperabilidade abre novas possibilidades para aplicações industriais, especialmente em ambientes que exigem colaboração entre múltiplos sistemas descentralizados (CHERVINSKI et al., 2023).

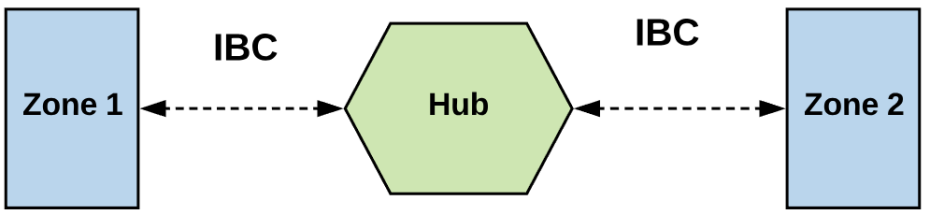


Figura 3.8 – Comunicação entre zonas via IBC. Fonte: Adaptado de Preethi Kasireddy (KASIREDDY, 2020).

## 3.6.2 Ferramenta Principal

### 3.6.2.1 Starport

O Starport configura-se como uma ferramenta de desenvolvimento altamente avançada e projetada para simplificar a criação e personalização de *blockchains* baseadas no Cosmos SDK. Com uma abordagem que abstrai a complexidade técnica, o Starport oferece um ambiente integrado que automatiza etapas críticas do processo de desenvolvimento, tornando-se uma solução indispensável para a construção de redes descentralizadas de alto desempenho. A ferramenta demonstra particular relevância em cenários acadêmicos e industriais que exigem soluções rápidas, customizáveis e altamente escaláveis (KANEVCHE et al., 2021).

A principal funcionalidade do Starport reside na sua capacidade de gerar, de forma automatizada, a estrutura básica de uma *blockchain*. Mediante a execução de comandos simplificados, o Starport cria redes completamente funcionais, incluindo configurações essenciais como contas, transações e mecanismos de governança. Esse nível de automação é especialmente vantajoso para desenvolvedores que não possuem perícia avançada no Cosmos SDK, permitindo-lhes focar na implementação de características específicas e personalizações adequadas às suas necessidades. Em contextos industriais, como sistemas de logística ou redes financeiras descentralizadas, essa simplificação reduz significativamente o tempo de desenvolvimento, otimizando recursos e acelerando a entrega de soluções (SURMONT; WANG; CUTSEM, 2023).

A customização constitui outro ponto fundamental do Starport, permitindo que desenvolvedores adaptem módulos pré-configurados ou criem novos componentes para atender a demandas específicas. A flexibilidade oferecida pela ferramenta possibilita, por exemplo, modificar o módulo de governança para implementar regras de votação customizadas ou criar módulos especializados para o gerenciamento de fluxos de trabalho industriais. Essa característica torna o Starport particularmente atrativo para aplicações voltadas à indústria 4.0, onde a necessidade de integração entre sistemas e o atendimento a requisitos específicos são frequentemente determinantes para o sucesso dos projetos (PAVLYSHYN et al., 2024).

Além disso, o Starport viabiliza a execução de redes de teste locais, um aspecto crucial para o desenvolvimento de *blockchains* seguras e funcionais. A capacidade de simular o comportamento da rede em um ambiente controlado permite identificar possíveis falhas e realizar ajustes antes da implantação em produção, assegurando maior confiabilidade e minimizando riscos. Essas redes de teste incluem todos os componentes essenciais, como o nó Tendermint e interfaces de consulta, criando um ambiente completo para experimentação e validação de soluções.

Outro atributo de destaque do Starport é sua integração com ferramentas modernas de infraestrutura, como Docker e *pipelines* de CI/CD (Integração e Entrega Contínuas). Essa compatibilidade permite que desenvolvedores implementem processos de automação robustos, garantindo maior eficiência e escalabilidade. Por exemplo, uma organização pode utilizar o Starport para gerar uma *blockchain* personalizada, empacotá-la em um contêiner Docker e implantá-la em um ambiente Kubernetes para operar em escala global. Essa integração atende às exigências de projetos industriais que demandam alta disponibilidade, segurança e facilidade de manutenção (SURMONT; WANG; CUTSEM, 2023).

A ferramenta também se destaca por sua capacidade de gerar documentação técnica automaticamente. Essa funcionalidade é de grande relevância no contexto acadêmico e empresarial, onde a documentação adequada é essencial para garantir a transparência, a auditabilidade e a interoperabilidade das soluções desenvolvidas. No âmbito da indústria 4.0, a geração automatizada de documentação contribui para o cumprimento de requisitos normativos e facilita a integração entre diferentes sistemas (PAVLYSHYN et al., 2024).

O impacto do Starport no ecossistema Cosmos é significativo, pois democratiza o acesso ao desenvolvimento de *blockchains*, possibilitando que profissionais de diferentes níveis de experiência tecnológica construam soluções customizadas. Ao acelerar o tempo de desenvolvimento e reduzir a complexidade técnica, o Starport não apenas contribui para a evolução das aplicações baseadas em *blockchain*, mas também consolida o Cosmos como uma plataforma preferencial para o desenvolvimento de redes descentralizadas personalizáveis. Assim, a ferramenta desempenha um papel estratégico ao promover a inovação tecnológica em um cenário global cada vez mais orientado à transformação digital e à integração de sistemas descentralizados na indústria moderna.

### 3.6.3 Aspectos Técnicos

#### 3.6.3.1 Estruturas de Rede no Cosmos

A arquitetura de rede do Cosmos é fundamentada em um modelo denominado *hub-and-zone*, que visa resolver desafios de escalabilidade e interoperabilidade enfrentados por *blockchains* tradicionais. Nesse modelo, os hubs, como o Cosmos Hub, funcionam como pontos centrais de interconexão, enquanto as zonas representam *blockchains* independentes conectadas a esses hubs. Cada zona é autônoma, podendo implementar suas próprias regras de governança, estrutura de dados e lógica de aplicação. Esse design permite que desenvolvedores criem *blockchains* específicas para diferentes casos de uso, sem comprometer a capacidade de comunicação com outras redes no ecossistema (PAVLYSHYN et al., 2024).

A abordagem *hub-and-zone* facilita a escalabilidade horizontal, pois novas zonas podem ser adicionadas sem impactar diretamente o desempenho das existentes. Essa característica torna o Cosmos ideal para aplicações que exigem a coexistência de múltiplas redes especializadas, como no setor industrial, onde sistemas de rastreamento de produção podem operar em sincronia com redes de gerenciamento financeiro. Além disso, os hubs garantem que a comunicação entre zonas seja eficiente e segura, centralizando a gestão das interações sem comprometer a autonomia de cada *blockchain* (ESSAID; KIM; JU, 2023).

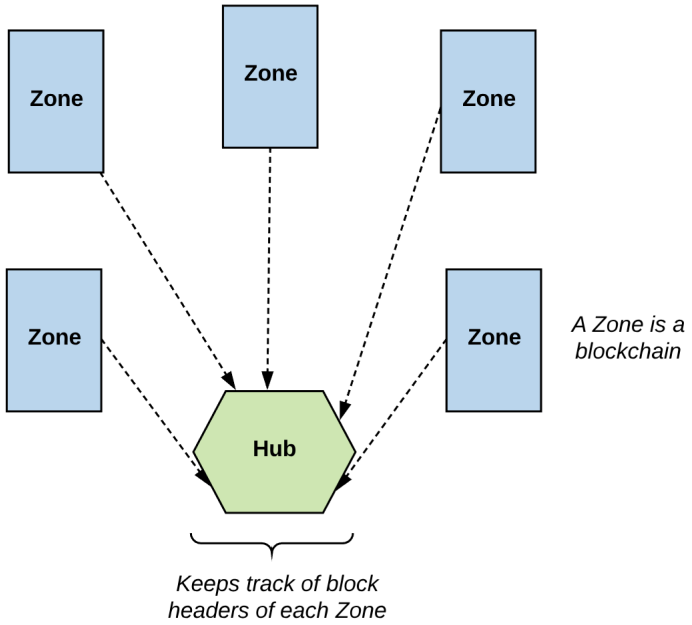


Figura 3.9 – Estrutura funcional de um hub no Cosmos. Fonte: Adaptado de Preethi Kasireddy (KASIREDDY, 2020).

#### 3.6.3.2 Mecanismos de Consenso (Tendermint)

O mecanismo de consenso do Cosmos é baseado no Tendermint Core, que combina a tolerância a falhas bizantinas (BFT) com o modelo *Proof of Stake* (PoS). O Tendermint BFT é projetado para garantir que a rede alcance consenso mesmo na presença de até um terço de validadores maliciosos ou inativos. Isso é alcançado através de um protocolo de votação que utiliza assinaturas criptográficas para validar transações e blocos.

No modelo PoS, os validadores são selecionados com base na quantidade de tokens apostados na rede, criando um incentivo econômico para comportamentos honestos. Esse mecanismo reduz drasticamente o consumo energético em comparação ao *Proof of Work* (PoW), tornando-o mais sustentável e eficiente. O Tendermint também oferece finalização imediata, ou seja, as transações são consideradas irreversíveis assim que um bloco é confirmado. Isso elimina o risco de reorganizações prolongadas na cadeia, como as que podem ocorrer em *blockchains* baseadas em PoW, tornando-o particularmente adequado para aplicações que exigem alta confiabilidade e baixa latência (AMOUSSOU-GUENOU et al., 2018).

A arquitetura do Tendermint é agnóstica à aplicação, o que significa que pode ser usada para construir qualquer tipo de *blockchain*. Isso o torna altamente adaptável para diversos cenários, desde redes financeiras descentralizadas até plataformas industriais que precisam de alta performance e segurança.

#### 3.6.3.3 Comunicação entre Blockchains

A comunicação entre *blockchains* no Cosmos é habilitada pelo protocolo Inter-Blockchain Communication (IBC), que permite a troca de dados, tokens e mensagens entre diferentes redes de forma segura e eficiente. O IBC é uma inovação central do Cosmos, possibilitando a criação de um ecossistema interoperável onde redes independentes podem colaborar sem a necessidade de intermediários (ESSAID; KIM; JU, 2023).

O funcionamento do IBC baseia-se em dois componentes principais: clientes leves e canais de comunicação. Os clientes leves são implementações de uma *blockchain* dentro de outra, permitindo que cada rede verifique transações e estados de forma autônoma. Já os canais estabelecem conexões seguras entre *blockchains*, garantindo que os dados transferidos sejam válidos e protegidos contra-ataques. Essa estrutura elimina pontos únicos de falha e mantém a segurança das interações *cross-chain*.

A flexibilidade do IBC permite que *blockchains* com diferentes arquiteturas e mecanismos de consenso se conectem ao Cosmos. Isso é particularmente vantajoso para casos de uso como cadeias de suprimentos, onde redes especializadas podem compartilhar dados de inventário, logística e transações financeiras em tempo real. Ao permitir a interoperabilidade sem comprometer a autonomia das redes, o IBC amplia significativamente o potencial de aplicações descentralizadas e posiciona o Cosmos como uma solução avançada para a indústria 4.0.

### 3.6.4 Comparação com Ethereum

O Cosmos Network e o Ethereum representam abordagens distintas para a concepção e implementação de *blockchains* e ecossistemas descentralizados, cada qual refletindo filosofias e objetivos técnicos próprios. Enquanto o Ethereum é amplamente reconhecido por sua capacidade de executar contratos inteligentes em uma única rede global, o Cosmos adota uma abordagem modular e distribuída, permitindo a criação de *blockchains* independentes, mas interoperáveis. Essas diferenças estruturais se traduzem em características técnicas e operacionais que impactam diretamente a escalabilidade, a interoperabilidade e o desempenho de ambas as plataformas.

#### 3.6.4.1 Arquitetura e Modularidade

A arquitetura do Ethereum é baseada em um modelo monolítico, no qual todas as aplicações compartilham os mesmos recursos computacionais e operam sobre uma única camada de execução. Essa abordagem garante uniformidade e padronização, facilitando a interação entre aplicações na mesma rede. No entanto, essa centralização também cria limitações em termos de escalabilidade e personalização. O Cosmos, em contraste, utiliza uma arquitetura modular baseada no modelo *hub-and-zone*, onde *blockchains* independentes (zonas) se conectam a hubs centrais, como o Cosmos Hub, para facilitar a interoperabilidade. Cada zona é totalmente autônoma, permitindo que seus desenvolvedores implementem regras específicas de governança,

execução e validação, enquanto preservam a capacidade de comunicação com outras redes. Essa modularidade promove um alto grau de flexibilidade, que é particularmente valioso em aplicações industriais que requerem soluções customizadas e independentes (CHAUHAN et al., 2018).

#### 3.6.4.2 Interoperabilidade

A interoperabilidade é um aspecto central onde o Cosmos apresenta vantagens claras em relação ao Ethereum. O Ethereum, mesmo com as melhorias introduzidas no Ethereum 2.0, continua enfrentando desafios para comunicação entre redes distintas, muitas vezes dependendo de soluções externas, como pontes centralizadas, que podem introduzir vulnerabilidades de segurança. O Cosmos, por outro lado, incorpora a interoperabilidade em sua estrutura fundamental por meio do protocolo Inter-Blockchain Communication (IBC). Este protocolo permite a troca nativa de dados, *tokens* e informações entre *blockchains*, de forma segura e sem intermediários. Tal capacidade torna o Cosmos especialmente adequado para cenários que exigem colaboração entre múltiplas redes, como cadeias de suprimentos descentralizadas ou ecossistemas financeiros que conectam várias jurisdições. A interoperabilidade garantida pelo IBC não apenas melhora a eficiência operacional, mas também amplia o escopo das aplicações possíveis no ecossistema Cosmos (ESSAID; KIM; JU, 2023).

#### 3.6.4.3 Escalabilidade e Eficiência

No Ethereum, todas as transações e execuções de contratos inteligentes ocorrem em uma única rede, o que pode levar a congestionamentos e taxas de transação elevadas durante períodos de alta demanda. Apesar da transição para o modelo PoS no Ethereum 2.0, a estrutura monolítica da rede continua sendo um fator limitante para a escalabilidade. Por outro lado, o Cosmos utiliza um modelo de escalabilidade horizontal, no qual novas *blockchains* podem ser adicionadas ao ecossistema sem impactar negativamente o desempenho das existentes. Essa abordagem distribui a carga de processamento entre diferentes redes, possibilitando um *throughput* significativamente maior e uma latência reduzida, características essenciais para aplicações que demandam alta performance e confiabilidade, como sistemas financeiros e industriais (CORTES-GOICOECHEA et al., 2024).

#### 3.6.4.4 Mecanismo de Consenso

Embora ambas as plataformas tenham adotado o modelo *Proof of Stake* em suas implementações mais recentes, o Cosmos apresenta características únicas com seu mecanismo Tendermint BFT. Este garante a finalização imediata das transações, eliminando o risco de reorganizações de blocos e oferecendo maior previsibilidade para desenvolvedores e usuários. No Ethereum, a finalização de transações, embora aprimorada com o PoS, pode ser menos imediata devido à estrutura de sua camada de execução. Além disso, o Tendermint é amplamente reconhecido por sua eficiência energética e simplicidade técnica, tornando-se uma escolha atrativa para

desenvolvedores que buscam implementar soluções seguras e de alto desempenho com custos operacionais reduzidos (AMOUSSOU-GUENOU et al., 2018).

#### 3.6.4.5 Aplicações e Usabilidade

O Ethereum se destaca por sua flexibilidade na execução de contratos inteligentes universais, mas sua arquitetura monolítica pode não ser ideal para projetos que demandam controle total sobre a infraestrutura da *blockchain*. O Cosmos, ao oferecer a possibilidade de construir *blockchains* específicas, permite que os desenvolvedores ajustem aspectos fundamentais, como mecanismos de governança e modelos econômicos, para atender a requisitos específicos. Essa flexibilidade é particularmente relevante para aplicações industriais e empresariais, onde as necessidades de personalização e controle são frequentemente essenciais para o sucesso do projeto. A capacidade de cada *blockchain* operar de forma independente dentro do Cosmos reduz potenciais conflitos de recursos e facilita a adaptação às demandas do setor (ASIF; HASSAN, 2023).

#### 3.6.4.6 Conclusão Comparativa

A análise comparativa entre o Cosmos Network e o Ethereum destaca duas abordagens distintas de design de *blockchain*. O Ethereum prioriza uma rede centralizada e acessível, ideal para a execução de contratos inteligentes globais, mas limitada em termos de escalabilidade e interoperabilidade. O Cosmos, com sua arquitetura modular e foco na comunicação entre *blockchains*, oferece uma solução mais adequada para aplicações que requerem personalização, escalabilidade e integração entre redes descentralizadas. Essas características tornam o Cosmos uma plataforma estratégica para a construção de *blockchains* industriais e empresariais, posicionando-se como uma alternativa robusta e inovadora para os desafios contemporâneos da indústria 4.0.

# 4 Experimentação Prática

## 4.1 Introdução

Neste capítulo, são descritos os passos para a implementação e configuração de uma rede privada *blockchain*, explorando os aspectos técnicos necessários para sua inicialização e operação. O foco está na criação e gerenciamento de nós, configuração de parâmetros essenciais e na automação da rede utilizando ferramentas específicas.

A implementação foi realizada utilizando duas abordagens: uma baseada no Ethereum com Geth e Docker, e outra utilizando o Cosmos SDK e Starport. São detalhados os procedimentos para configuração, inicialização e manutenção da rede, destacando os desafios técnicos enfrentados e as estratégias utilizadas para garantir a estabilidade e segurança do ambiente configurado.

## 4.2 Configuração da Rede Privada Ethereum

A criação de uma rede privada utilizando Ethereum e Geth tem o objetivo de simular o funcionamento de uma *blockchain* em ambiente controlado. Essa experiência prática proporciona uma compreensão profunda de como os elementos técnicos de uma *blockchain* são implementados, desde a configuração do bloco gênesis até a operação dos nós mineradores. Para esta rede, utilizou-se o Geth (um cliente Ethereum escrito em Go) em conjunto com Docker, a fim de permitir uma configuração eficiente e modular dos nós da rede (Figura 4.1).

### 4.2.1 Bloco Gênesis e Arquivo de Configuração genesis.json

No que se referem à *blockchain* Ethereum, o primeiro passo para formar a rede privada foi o bloco gênesis, que define as condições iniciais para a implementação da *blockchain*. A formação do bloco gênesis para a *blockchain* Ethereum é realizada no arquivo genesis.json. Neste arquivo, são criadas as principais condições para a futura integração da rede, que, ao se combinar com o *software* de mineradores e clientes de nó completo ou nó finito, define o funcionamento técnico da rede.

**Chain ID**

A rede privada foi configurada com o valor 3456 no campo chain id, o que garante uma identificação única para a rede. Esse valor é crucial para evitar conflitos com outras redes públicas ou privadas do Ethereum, assegurando que transações realizadas em uma rede não possam ser replicadas em outra. Esse isolamento é importante no contexto industrial para garantir que transações em uma rede privada não afetem sistemas públicos, preservando a integridade e a segurança dos dados.

### Atualizações de Protocolo

As principais atualizações do Ethereum, como Byzantium, Constantinople e Petersburg, foram ativadas desde o bloco gênesis. A instalação destas atualizações assegura que as transações sejam feitas com base nas leis de consenso mais seguras mais recentes em vigor no Ethereum, garantindo a segurança e a eficácia da rede. Na indústria, onde a coesão e a segurança torna-se uma necessidade, ter uma rede segura e contínua é imperativo por meio da instalação das versões de protocolo mais recentes.

### Dificuldade

A dificuldade foi ajustada para 1 para possibilitar uma mineração de blocos rápida no ambiente de testes. Essa configuração é crucial para validação rápida de transações e criação de blocos, algo fundamental em simulações que demandam respostas rápidas.

### Limite de Gas

O limite do *gas* foi ajustado para 12.000.000, e isso permite a inclusão de transações complexas em um único bloco. *Gas*, no caso do Ethereum, refere-se ao custo computacional de transações e contratos inteligentes. As redes da indústria 4.0, que se preocupam com grandes conjuntos de dados, como a execução de contratos inteligentes que monitoram a produção e distribuição de suprimentos entre os contratos, têm requisitos elevados de limite de *gas* para um processamento seguro e eficiente de várias transações.

```json
{
  "config": {
    "chainId": 3456,
    "homesteadBlock": 0,
    "eip150Block": 0,
    "eip155Block": 0,
    "eip158Block": 0,
    "byzantiumBlock": 0,
    "constantinopleBlock": 0,
    "petersburgBlock": 0,
    "ethash": {}
  },
  "difficulty": "1",
  "gasLimit": "12000000",
  "alloc": {}
}
```

Figura 4.1 – Exemplo de configuração do bloco gênesis no arquivo genesis.json.

### 4.2.2 Arquivo .env e Configuração de Variáveis

O uso de variáveis sensíveis, como chaves privadas e endereços de nós, no arquivo .env permite uma configuração centralizada e eficiente da rede. Todas as variáveis de ambiente são, assim, fáceis e seguras de gerenciar, especialmente com informações altamente críticas em um ambiente industrial. Manter todas as variáveis de ambiente em um único local significa que a configuração da rede pode ser modificada rapidamente, sem a necessidade de reconfigurar individualmente cada nó.

Além disso, o processo de automação é seguro, já que nenhuma informação sensível é transferida em scripts ou logs, algo ainda mais relevante em sistemas industriais, onde o controle de acesso estritamente seguro é essencial. A facilidade de manipular as variáveis de ambiente também permite a escalabilidade da rede, facilitando a adição ou remoção de nós conforme as necessidades operacionais (Figura 4.2).

```bash
NETWORK_ID=3456
ACCOUNT_PASSWORD=<senha>
```

Figura 4.2 – Defininfo variáveis de ambiente.

`ACCOUNT_PASSWORD`: A senha das contas foi armazenada de forma segura para ser utilizada durante a criação das contas de nós mineradores.

`NETWORK_ID`: O valor 3456 foi utilizado aqui para garantir que todos os nós da rede usassem o mesmo ID de rede, permitindo a conectividade e a comunicação correta entre os nós.

### 4.2.3 Criação do Dockerfile e Automação da Inicialização

O Docker permitiu a configuração automatizada dos nós da rede Ethereum, tornando o desenvolvimento modular e independente de outras redes. No decorrer deste experimento, a instalação e ajuste do Geth foram efetuados para garantir uma configuração uniforme e eficaz em cada nó. Neste cenário, essa abordagem proporciona diversos benefícios, pois na era da indústria 4.0, é crucial que os sistemas possam ser flexíveis para se ajustarem às variações das operações industriais.

Esta estratégia possibilita a modularidade na inclusão de novos nós na rede sem a exigência de interrupções, tornando o sistema mais adaptável e capaz de responder à demanda operacional em ascensão no cenário industrial. Adicionalmente, a capacidade de portabilidade das imagens Docker permite a replicação dos cenários de teste em qualquer tipo de infraestrutura, seja em servidores locais ou na nuvem. Isso torna o desenvolvimento e os testes de novas soluções industriais baseadas em *blockchain* mais flexíveis e ágeis (TEISSERENC; SEPASGOZAR, 2021), (Figura 4.3).

```bash
FROM ethereum/client-go:v1.10.1

ARG ACCOUNT_PASSWORD

COPY genesis.json .

RUN geth init ./genesis.json \
    && rm -f ~/.ethereum/geth/nodekey \
    && echo ${ACCOUNT_PASSWORD} > ./password.txt \
    && geth account new --password ./password.txt \
    && rm -f ./password.txt

ENTRYPOINT ["geth"]
```

Figura 4.3 – Dockerfile para inicializar a rede Ethereum usando Geth.

**Base Image**

A imagem base escolhida foi a ethereum/client-go:v1.10.1, que é uma versão estável do Geth.

**Inicialização da Blockchain**

A *blockchain* foi inicializada utilizando o arquivo genesis.json com o comando geth init ./genesis.json. Isso garantiu que todos os nós compartilhassem o mesmo bloco gênesis.

**Criação de Contas**

Utilizando a senha armazenada no arquivo .env, foram criadas contas para os nós mineradores. Este processo automatizado via Docker garantiu que todos os nós fossem inicializados com as mesmas configurações, reduzindo a margem de erro e facilitando a replicação da rede em diferentes ambientes.

### 4.2.4 Configuração do Bootnode e Enode

Definir um *bootnode* e usar enodes foram passos críticos para descobrir pares e estabelecer conexões entre os nós. O *bootnode* atua como ponte de entrada para qualquer novo nó que queira acessar a rede, portanto, ele permite a criação de topologia *peer-to-peer* descentralizada.

Para a indústria 4.0, essa topologia é essencial para que sistemas distribuídos e autônomos possam conversar e tomar decisões em conjunto. Em outras palavras, a topologia garante a resistência. Assim, cada nó recebeu todas as informações necessárias para se conectar a outros nós de forma segura, estável e descentralizada. Dessa maneira, eles foram capazes de compartilhar informações e validar transações. Um benefício da estrutura P2P para sistemas é que máquinas e dispositivos interconectados em uma fábrica podem compartilhar a decisão com pelo menos dois nós. Consequentemente, se um ponto de controle local falhar, ele não interromperá a operação geral, o que leva à robustez e resiliência, uma vez que a operação pode continuar por um único

canal (HOSSAIN; BADSHA; SHEN, 2020).

1. Geração da Chave do *Bootnode*

   O comando bootnode -genkey bootnode.key foi utilizado para gerar a chave criptográfica única do *bootnode*. Essa chave é crucial para a identificação do nó dentro da rede (Figura 4.4).

```bash
bootnode –genkey bootnode.key
```

Figura 4.4 – Comando para gerar a chave criptográfica do *bootnode*.

2. Geração do Enode

   O identificador único do *bootnode*, conhecido como enode, foi gerado utilizando o comando bootnode -nodekeyhex <nodekeyhex-from-file> -writeaddress (Figura 4.5).

```bash
bootnode –nodekeyhex <nodekeyhex> –writeaddress
```

Figura 4.5 – Formato do identificador enode com IP e porta.

   O enode resultante foi então utilizado para conectar os nós mineradores ao *bootnode*. O enode segue o formato enode://ENODE-value@IP:PORT, onde o valor do ENODE é a chave do nó e o IP/PORT refere-se ao endereço de rede. No contexto da rede privada, o IP utilizado foi o endereço local do *bootnode* (Figura 4.6).

```php
enode://<ENODE>@<IP>:<PORT>
```

Figura 4.6 – Comando para gerar o enode a partir da chave do nó.

### 4.2.5 Arquivo docker-compose.yml e Conectividade da Rede

O docker-compose.yml foi usado para orquestrar a inicialização de múltiplos nós na rede para garantir que eles estivessem adequadamente conectados. Isso permitiu que todos os nós fossem iniciados e conectados sem intervenção manual, um requisito essencial para ambientes industriais onde é necessário que eles executem atividades continuamente. O Docker Compose

é adequado para a escalabilidade, pois traz flexibilidade para a rede, o que significa que a rede pode crescer à medida que a operação industrial expandir a produção.

A habilidade de administrar a conectividade de rede de maneira dinâmica e modular assegura que sistemas industriais baseados em *blockchain* possam se desenvolver sem comprometer a eficiência ou a segurança. A adaptabilidade é benéfica em contextos industriais, pois assegura que as operações possam ser ajustadas conforme a demanda, seja por novos requisitos de produção ou mudanças nos processos de geração. Segue uma lista de alguns aspectos notáveis da configuração:

```
services:
  mybootnode:
    hostname: mybootnode
    platform: linux/arm64/v8
    env_file:
      - .env
    build:
      context: .
      args:
        - ACCOUNT_PASSWORD=${ACCOUNT_PASSWORD}
    command:
      --nodekeyhex="d8a72d2f214c7813ab24407d550a0fee0262e595e8ab6
    6c2d5c4af4291001b8e" --nodiscover --ipcdisable
      --networkid=${NETWORK_ID} --netrestrict="192.168.120.0/24"
    networks:
      priv-eth-net:
        ipv4_address: 192.168.120.2

  miner-1:
    hostname: miner-1
    platform: linux/arm64/v8
    env_file:
      - .env
    build:
      context: .
      args:
        - ACCOUNT_PASSWORD=${ACCOUNT_PASSWORD}
    command: --bootnodes="enode://2bd6c478d1922fd3f4b99944c5f54ac4a04
8e2cdbf5f09827a07b62119f2f0e30fc2b4c802818cdfbfd6bf4f36b7ecf5a908b966
d1dc16c25fdb2723d9325f67@192.168.120.2:30301" --mine
    --miner.threads=1 --networkid=${NETWORK_ID} --http --http.addr
    "0.0.0.0" --http.port 8545 --http.api "eth,net,web3,personal"
    --allow-insecure-unlock --unlock 0 --password
```

```
    /root/.ethereum/password.txt --netrestrict="192.168.120.0/24"
29    volumes:
30      - ./password.txt:/root/.ethereum/password.txt
31    networks:
32      priv-eth-net:
33        ipv4_address: 192.168.120.3
34    ports:
35      - "8545:8545"
36      - "30303:30303"
37
38  miner-2:
39    hostname: miner-2
40    platform: linux/arm64/v8
41    env_file:
42      - .env
43    build:
44      context: .
45      args:
46        - ACCOUNT_PASSWORD=${ACCOUNT_PASSWORD}
47    command:
        --bootnodes="enode://2bd6c478d1922fd3f4b99944c5f54ac4a048e2cdb
48  f5f09827a07b62119f2f0e30fc2b4c802818cdfbfd6bf4f36b7ecf5a908b966d1dc1
49  6c25fdb2723d9325f67@192.168.120.2:30301" --mine --miner.threads=1
    --networkid=${NETWORK_ID} --http --http.addr "0.0.0.0"
    --http.port 8546 --http.api "eth,net,web3,personal"
    --allow-insecure-unlock --unlock 0 --password
    /root/.ethereum/password.txt --netrestrict="192.168.120.0/24"
50    volumes:
51      - ./password.txt:/root/.ethereum/password.txt
52    networks:
53      priv-eth-net:
54        ipv4_address: 192.168.120.4
55    ports:
56      - "8546:8546"
57      - "30304:30303"
58
59  miner-3:
60    hostname: miner-3
61    platform: linux/arm64/v8
62    env_file:
63      - .env
64    build:
```

```
65        context: .
66        args:
67          - ACCOUNT_PASSWORD=${ACCOUNT_PASSWORD}
68      command:
          --bootnodes="enode://2bd6c478d1922fd3f4b99944c5f54ac4a048e2cdb
69  f5f09827a07b62119f2f0e30fc2b4c802818cdfbfd6bf4f36b7ecf5a908b966d1dc1
70  6c25fdb2723d9325f67@192.168.120.2:30301" --mine --miner.threads=1
    --networkid=${NETWORK_ID} --http --http.addr "0.0.0.0"
    --http.port 8547 --http.api "eth,net,web3,personal"
    --allow-insecure-unlock --unlock 0 --password
    /root/.ethereum/password.txt --netrestrict="192.168.120.0/24"
71      volumes:
72        - ./password.txt:/root/.ethereum/password.txt
73      networks:
74        priv-eth-net:
75          ipv4_address: 192.168.120.5
76      ports:
77        - "8547:8547"
78        - "30305:30303"
79
80    miner-4:
81      hostname: miner-4
82      platform: linux/arm64/v8
83      env_file:
84        - .env
85      build:
86        context: .
87        args:
88          - ACCOUNT_PASSWORD=${ACCOUNT_PASSWORD}
89      command:
          --bootnodes="enode://2bd6c478d1922fd3f4b99944c5f54ac4a048e2cdb
90  f5f09827a07b62119f2f0e30fc2b4c802818cdfbfd6bf4f36b7ecf5a908b966d1dc1
91  6c25fdb2723d9325f67@192.168.120.2:30301" --mine --miner.threads=1
    --networkid=${NETWORK_ID} --http --http.addr "0.0.0.0"
    --http.port 8548 --http.api "eth,net,web3,personal"
    --allow-insecure-unlock --unlock 0 --password
    /root/.ethereum/password.txt --netrestrict="192.168.120.0/24"
92      volumes:
93        - ./password.txt:/root/.ethereum/password.txt
94      networks:
95        priv-eth-net:
96          ipv4_address: 192.168.120.6
```

```
97      ports:
98        - "8548:8548"
99        - "30306:30303"
100
101   miner-5:
102     hostname: miner-5
103     platform: linux/arm64/v8
104     env_file:
105       - .env
106     build:
107       context: .
108       args:
109         - ACCOUNT_PASSWORD=${ACCOUNT_PASSWORD}
110     command:
          --bootnodes="enode://2bd6c478d1922fd3f4b99944c5f54ac4a048e2cdb
111 f5f09827a07b62119f2f0e30fc2b4c802818cdfbfd6bf4f36b7ecf5a908b966d1dc1
112 6c25fdb2723d9325f67@192.168.120.2:30301" --mine --miner.threads=1
    --networkid=${NETWORK_ID} --http --http.addr "0.0.0.0"
    --http.port 8549 --http.api "eth,net,web3,personal"
    --allow-insecure-unlock --unlock 0 --password
    /root/.ethereum/password.txt --netrestrict="192.168.120.0/24"
113     volumes:
114       - ./password.txt:/root/.ethereum/password.txt
115     networks:
116       priv-eth-net:
117         ipv4_address: 192.168.120.7
118     ports:
119       - "8549:8549"
120       - "30307:30303"
121
122 networks:
123   priv-eth-net:
124     driver: bridge
125     ipam:
126       config:
127         - subnet: 192.168.120.0/24
```

docker-compose.yml

### Serviço do Bootnode

O *bootnode* foi definido como um serviço no Docker Compose, com as variáveis de ambiente configuradas no arquivo .env. O *bootnode* foi configurado para não participar da

mineração, mas apenas para atuar como ponto de descoberta.

**Serviços dos Nós Mineradores**

Cada nó minerador foi configurado para se conectar ao *bootnode* utilizando o enode gerado. Os nós mineradores foram nomeados sequencialmente (miner-1, miner-2, miner-3, miner-4, miner-5), cada um deles executa o processo de mineração de blocos.

**Rede Privada**

Todos os serviços foram conectados em uma rede *bridge* chamada priv-eth-net, garantindo que os nós pudessem se comunicar internamente.

## 4.3 Execução da Rede e Mineração

Após a configuração dos arquivos, a rede foi iniciada com os comandos docker-compose build e docker-compose up. O processo de construção garantiu que todas as imagens Docker necessárias fossem criadas, e a execução ativou os contêineres de cada nó da rede. A rede começou a operar com todos os nós conectados ao *bootnode*, e o processo de mineração foi iniciado (Figura 4.7).

```bash
docker-compose up --build
```

Figura 4.7 – Comando para construir e iniciar a rede usando Docker Compose.

### 4.3.1 Validação de Blocos e Sincronização de Nós

Após a configuração, a rede iniciou o processo de verificação de transações e produção de blocos. Os nós de mineração verificaram cada operação conforme as normas estabelecidas no arquivo genesis.json, assegurando a salvaguarda e a atualização constante do *ledger* distribuído. Portanto, a sincronização dos nós foi fundamental para assegurar que todos os participantes da rede estivessem em conformidade com a *blockchain*.

A abordagem implementada por meio de *blockchain* é a validação distribuída, essa conduta oferece um nível extra de segurança, já que, uma vez que eles foram inseridos no *blockchain*, as transações individuais não podem ser modificadas. Tal flexibilidade tornou-se desejável para cadeias de suprimentos e sistemas de automação industrial modernos, uma vez que a tomada de decisões com base nessas transações deve ser confiável e a rastreabilidade dos materiais e produtos deve ser segura. Deve-se revisar constantemente as transações na indústria 4.0 para garantir a integridade das operações industriais e a ausência de fraude (GARROCHO, 2022).

### 4.3.2 Realização de Transações

Com a rede em pleno funcionamento, foi possível interagir com os nós utilizando o console JavaScript do Geth. Primeiramente, criaram-se novas contas e transferiu-se ether entre elas. O comando utilizado para enviar ether foi (Figura 4.8):

```javascript
eth.sendTransaction({
    from: eth.accounts[0],
    to: eth.accounts[1],
    value: web3.toWei(1, "ether")
})
```

Figura 4.8 – Comando para enviar uma transação Ethereum.

As transações foram validadas pela rede, com os mineradores gerando blocos e incluindo as transações. As informações detalhadas sobre as transações e blocos foram obtidas com o comando, utilizando o *hash* da transação que é gerado após sua conclusão (Figura 4.9):

```js
eth.getTransaction("<hash-da-transação>")
```

Figura 4.9 – Comando para recuperar uma transação pelo *hash*.

Os detalhes de cada transação, incluindo o *hash* do bloco, o valor transferido e as taxas de gas, foram devidamente registrados na *blockchain*, demonstrando a imutabilidade e a segurança das transações realizadas.

### 4.3.3 Transações Automáticas

Além das transações manuais, para simular um ambiente industrial com alta carga transacional, foi desenvolvido um *script* em JavaScript, utilizando a biblioteca Web3.js, que automatiza a criação de contas para cada minerador, seu desbloqueio e financiamento pela conta mestre. Além disso, o *script* realiza transações regulares entre essas contas, simulando um fluxo contínuo de transações e permitindo o monitoramento da performance da rede em cenários de alta demanda.

## 4.4 Configuração da Rede Privada Cosmos

Nesta seção, apresenta-se a experimentação prática realizada para validar a implementação de uma *blockchain* customizada para a indústria 4.0, utilizando o Cosmos SDK, a linguagem

Go e a ferramenta Starport. O objetivo principal foi analisar o desempenho e a viabilidade da implementação de uma rede *blockchain* privada voltada para a automação de processos industriais, explorando sua escalabilidade, tempo de confirmação de transações e segurança.

### 4.4.1 Configuração do Ambiente

A primeira etapa para a implementação da *blockchain* envolveu a configuração do ambiente de desenvolvimento. Essa etapa é essencial para garantir que todas as dependências necessárias estejam corretamente instaladas e configuradas, permitindo a execução fluida do projeto.

Inicialmente, foi utilizado um ambiente baseado no sistema operacional Ubuntu 22.04 LTS, por sua estabilidade e compatibilidade com as ferramentas utilizadas. A linguagem de programação principal adotada foi o Go, gerenciado por meio dos arquivos go.mod e go.sum, os quais definem e controlam as dependências do projeto. Para a estruturação da *blockchain*, utilizou-se o Cosmos SDK, uma estrutura que permite a implementação de *blockchains* personalizadas de forma modular.

O mecanismo de consenso adotado foi o Tendermint BFT, que garante eficiência e segurança na validação de transações e criação de blocos. Por fim, o Starport CLI foi utilizado como ferramenta principal para a criação e automação do desenvolvimento da *blockchain*, oferecendo uma interface intuitiva e eficiente para a geração e configuração dos componentes do sistema.

### 4.4.2 Inicialização do Projeto

Após a configuração adequada do ambiente de desenvolvimento, iniciou-se o processo de criação da *blockchain* por meio do comando apresentado na Figura 4.10. Esse comando tem a função de estruturar automaticamente o projeto, gerando os diretórios e arquivos essenciais para a sua organização e funcionamento.

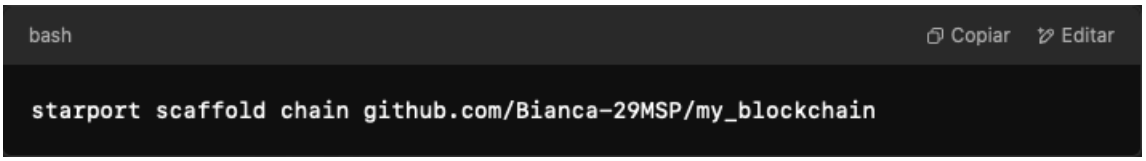


Figura 4.10 – Comando utilizado para a criação da estrutura inicial do projeto de *blockchain*.

A execução desse comando resulta na criação de uma estrutura modular que facilita a implementação e manutenção do sistema. Entre os elementos gerados, destaca-se o diretório cmd/, que contém os comandos necessários para a execução da *blockchain*, permitindo sua inicialização e gerenciamento. Além disso, é criado o arquivo config.yml, onde são definidas as configurações da rede, incluindo parâmetros como tempo de bloqueio e critérios de consenso, garantindo a estabilidade e a eficiência do sistema.

Outro componente fundamental é o diretório x/, no qual são armazenados os módulos personalizados responsáveis por implementar a lógica de negócio da *blockchain*, possibilitando a adaptação da rede às necessidades específicas do projeto. Complementando a estrutura, há o diretório vue/, destinado à interface web, permitindo a interação do usuário com a rede por meio de um ambiente gráfico intuitivo.

A partir dessa estrutura inicial, a implementação da *blockchain* pode ser conduzida de maneira organizada, garantindo um desenvolvimento escalável e alinhado às diretrizes da plataforma Cosmos SDK.

### 4.4.3 Configuração da Rede Blockchain

A configuração da rede *blockchain* foi realizada através do arquivo config.yml, responsável por definir os seguintes parâmetros essenciais:

- Contas iniciais: Duas contas padrão foram criadas, alice e bob, com diferentes saldos de tokens e stakes

```yaml
accounts:
  - name: alice
    coins: ["20000token", "200000000stake"]
  - name: bob
    coins: ["10000token", "100000000stake"]
```

Figura 4.11 – Comando usado para criar a estrutura inicial do seu projeto de *blockchain*.

- Validador inicial: Alice foi definida como validadora com uma quantia inicial de stake:

```yaml
validator:
  name: alice
  staked: "100000000stake"
```

Figura 4.12 – Configuração presente no arquivo config.yml

- Configuração do cliente: O cliente possui suporte a OpenAPI e Vuex para gerenciamento da interface:

```yaml
client:
  openapi:
    path: "docs/static/openapi.yml"
  vuex:
    path: "vue/src/store"
```

Figura 4.13 – Configuração presente no arquivo config.yml

- Faucet: Bob tem permissão para distribuir pequenas quantias de tokens para facilitar testes na rede:

```
faucet:
  name: bob
  coins: ["5token", "100000stake"]
```

Figura 4.14 – Configuração presente no arquivo config.yml

Com essa configuração, a *blockchain* foi iniciada com o comando:

```
bash                                                    Copiar  Editar

starport chain serve
```

Figura 4.15 – Comando de inicialização da *blockchain*.

Esse comando instala automaticamente todas as dependências necessárias, compila o código e inicia a execução da rede em ambiente local, permitindo a interação e testes da infraestrutura implementada.

## 4.5 Execução da Rede

### 4.5.1 Realização de Transações

A execução de transações dentro da *blockchain* desenvolvida permite a movimentação de ativos entre diferentes contas. Para efetuar uma transferência de *tokens*, utilizamos o comando 'my_blockchain tx bank send', no qual é especificado o remetente, o destinatário e a quantidade de *tokens* a ser transferida. Ao executar o comando, a transação é registrada e processada pela rede, garantindo que os valores sejam debitados da conta de origem e creditados na conta de destino. O comando executado seria:

```
my_blockchain tx bank send <remetente> <destinatário> <quantidade> --chain-id=<id-da-rede>
```

Figura 4.16 – Comando de realização de transações dentro da *blockchain*.

Uma vez que a transação é submetida, o mecanismo de consenso da *blockchain* verifica a validade da operação, incluindo a existência de saldo suficiente na conta remetente e a autenticação dos participantes envolvidos. Se validada com sucesso, a transação é incluída no próximo bloco da cadeia, tornando-se imutável e permanentemente registrada na rede.

# 5 Resultados

## 5.1 Análise dos Resultados

Este capítulo apresenta uma análise sistemática e comparativa dos resultados experimentais obtidos a partir da implementação das redes privadas Ethereum e Cosmos. A análise é fundamentada em métricas quantitativas que permitem avaliar o desempenho, a eficiência e a robustez das plataformas *blockchain* estudadas. O protocolo experimental foi estruturado para possibilitar a mensuração de parâmetros críticos, incluindo a latência de rede, o tempo de processamento de blocos, o *throughput* transacional e a distribuição de carga entre os nós mineradores (Ethereum) e validadores (Cosmos).

A metodologia adotada segue uma abordagem experimental comparativa, cuja estrutura analítica organiza-se em três seções principais: (i) análise paramétrica da rede Ethereum, com ênfase na avaliação do desempenho dos mineradores e nas correlações estatísticas entre as variáveis mensuradas; (ii) análise paramétrica da rede Cosmos, focalizando as métricas específicas do ecossistema Tendermint e o comportamento dos validadores; e (iii) análise comparativa entre as plataformas, fundamentada em critérios objetivos de desempenho e escalabilidade.

## 5.2 Resultados na Rede Ethereum

### 5.2.1 Análise Paramétrica do Desempenho dos Mineradores

A rede Ethereum experimental foi configurada com cinco mineradores, cada um operando sob condições controladas, porém com variações inerentes às características de *hardware* e à topologia de rede. A tabela 5.1 apresenta uma síntese quantitativa do desempenho observado para cada minerador, discriminando os tempos médios, mínimos e máximos para a extração de blocos.

| Minerador | Tempo Médio (s) | Tempo Mínimo (s) | Tempo Máximo (s) |
|---|---|---|---|
| Minerador 1 | 141,91 | 29,10 | 396,00 |
| Minerador 2 | 159,54 | 26,80 | 499,00 |
| Minerador 3 | 142,43 | 27,30 | 402,00 |
| Minerador 4 | 154,34 | 26,80 | 467,00 |
| Minerador 5 | 151,34 | 25,90 | 746,00 |

Tabela 5.1 – Análise temporal da extração de blocos por minerador

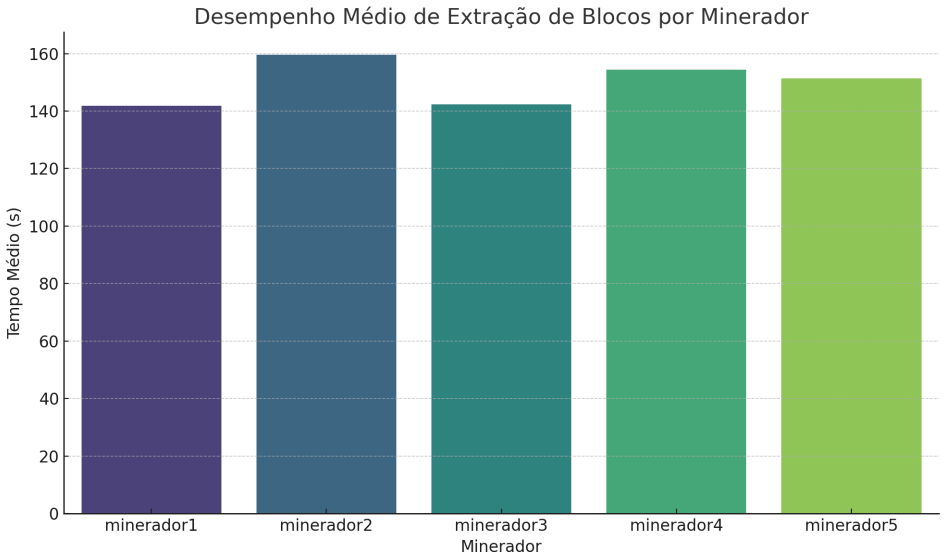


Figura 5.1 – Distribuição comparativa dos tempos médios de extração de blocos

A análise comparativa dos tempos médios de extração de blocos revela uma diferença estatisticamente significativa entre o desempenho do Minerador 1 e do Minerador 2, representando uma variação de aproximadamente 12,4%. Considerando que as condições experimentais foram controladas para minimizar variáveis exógenas, esta diferença sugere a existência de fatores endógenos relacionados à configuração e operação dos mineradores.

A análise dos valores extremos (mínimos e máximos) revela padrões ainda mais distintivos. O Minerador 5, apesar de apresentar o menor tempo mínimo de extração, também registrou o maior tempo máximo, evidenciando uma instabilidade operacional significativa. Esta amplitude nos valores de tempo de extração contrasta com a amplitude consideravelmente menor observada no Minerador 3, sugerindo que este último apresenta operação mais estável e previsível.

| Minerador | Características Operacionais |
|---|---|
| Minerador 1 | Apresenta o melhor desempenho médio (141,91s), com estabilidade operacional intermediária evidenciada pela amplitude de 366,90s entre os valores extremos. |
| Minerador 2 | Demonstra o desempenho médio mais baixo (159,54s), com amplitude considerável entre valores extremos (472,20s), sugerindo potenciais ineficiências na configuração ou operação. |
| Minerador 3 | Exibe consistência operacional superior, com tempo médio próximo ao melhor valor observado (142,43s) e menor amplitude entre extremos (374,70s), indicando maior previsibilidade. |
| Minerador 4 | Apresenta desempenho intermediário (154,34s) com amplitude significativa entre valores extremos (440,20s), sugerindo oscilações operacionais moderadas. |
| Minerador 5 | Caracteriza-se por alta instabilidade operacional, evidenciada pela amplitude máxima entre extremos (720,10s), apesar de tempo médio intermediário (151,34s). |

Tabela 5.2 – Análise qualitativa das características operacionais dos mineradores

### 5.2.2 Análise da Relação entre Latência e Eficiência Operacional

A investigação da relação entre a latência de rede e a eficiência operacional dos mineradores constitui um elemento fundamental para a compreensão dos fatores limitantes do desempenho global do sistema. Os dados experimentais permitiram quantificar esta relação, conforme apresentado na tabela 5.3.

| Minerador | Latência Média (ms) | Tempo Médio de Extração (s) |
|---|---|---|
| Minerador 1 | 112,92 | 141,91 |
| Minerador 2 | 358,10 | 159,54 |
| Minerador 3 | 108,45 | 142,43 |
| Minerador 4 | 112,58 | 154,34 |
| Minerador 5 | 122,28 | 151,34 |

Tabela 5.3 – Correlação entre latência de rede e eficiência operacional por minerador

A análise estatística da correlação entre estas variáveis resultou em um coeficiente de Pearson de 0,72, indicando uma associação positiva forte. Este resultado corrobora a hipótese de que a latência de rede constitui um fator determinante para a eficiência operacional dos mineradores, afetando diretamente o tempo necessário para a extração de blocos.

O Minerador 2, que apresentou a maior latência média, significativamente superior aos demais, também registrou o maior tempo médio de extração. Analogamente, o Minerador 3, com a menor latência média, demonstrou um dos melhores desempenhos em termos de tempo médio de extração. Esta correspondência consistente entre as variáveis analisadas reforça a significância estatística da correlação identificada.

### 5.2.3 Análise do Throughput Transacional

A avaliação do desempenho de redes *blockchain* exige uma análise detalhada do *throughput* transacional, definido como o número de transações processadas por unidade de tempo. No contexto desta experimento, a rede Ethereum foi submetida a uma análise temporal abrangente, revelando padrões complexos de processamento transacional ao longo de um ciclo de 24 horas.

Os resultados evidenciam um *throughput* médio global de 0,14 transações por segundo (TPS), com uma variabilidade significativa que oscila entre 0,0167 TPS e 4,08 TPS. Esta amplitude demonstra a natureza dinâmica e não homogênea da carga transacional, característica de sistemas *blockchain* descentralizados.

A decomposição temporal do *throughput* revela três regimes distintos de atividade:

1. **Período de Alta Atividade** (08h–11h): caracterizado por uma densidade transacional superior, com média entre 0,20 e 0,40 TPS e pico máximo às 08h (4,08 TPS).
2. **Período de Atividade Intermediária** (00h, 09h, 12h–19h, 23h): valores entre 0,13 e 0,23 TPS.
3. **Período de Baixa Atividade** (02h, 04h, 06h, 20h–21h): com médias inferiores a 0,11 TPS, atingindo o mínimo às 04h (0,07 TPS).

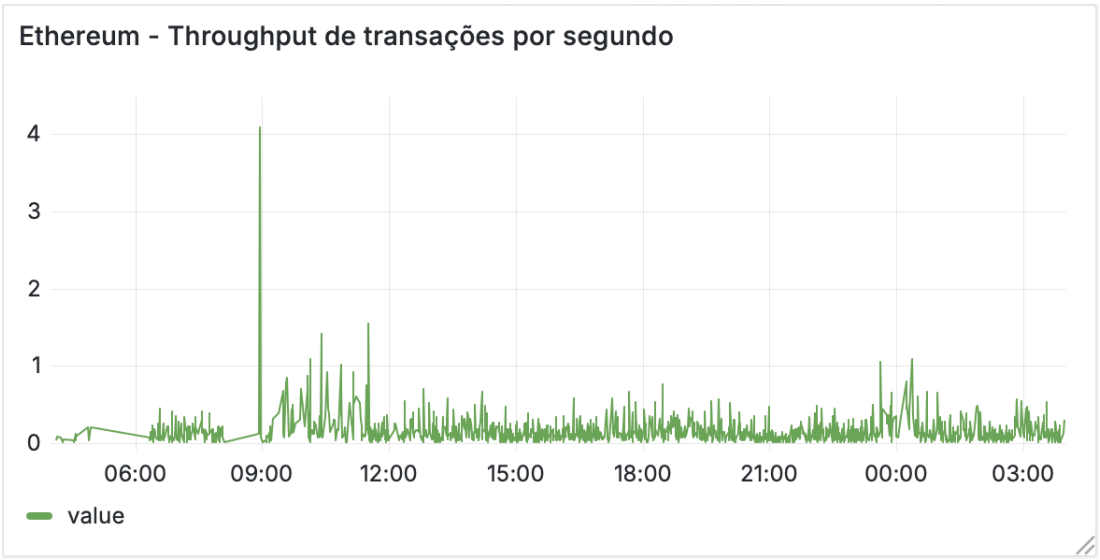


Figura 5.2 – Variação do throughput transacional ao longo de 24 horas

| Minerador | Throughput Médio (TPS) | Máximo (TPS) | Mediana (TPS) |
|---|---|---|---|
| Minerador 1 | 0,137 | 1,08 | 0,100 |
| Minerador 2 | 0,136 | 4,08 | 0,083 |
| Minerador 3 | 0,139 | 0,92 | 0,100 |
| Minerador 4 | 0,146 | 0,92 | 0,100 |
| Minerador 5 | 0,138 | 1,55 | 0,083 |

Tabela 5.4 – Análise estatística do throughput transacional por minerador

A análise comparativa do desempenho individual dos mineradores evidencia uma notável homogeneidade, com *throughput* médio variando entre 0,136 TPS (Minerador 2) e 0,146 TPS (Minerador 4), representando uma variação percentual inferior a 7,4%. Esta uniformidade sugere um balanceamento de carga eficiente, elemento crucial em arquiteturas de sistemas distribuídos.

A distribuição estatística revelou uma assimetria positiva, evidenciada pela discrepância entre a média (0,14 TPS) e a mediana (0,10 TPS) do *throughput* global. Esta característica indica que o comportamento típico da rede corresponde a valores moderadamente inferiores à média aritmética, com elevações periódicas que influenciam significativamente a métrica global.

É imperativo contextualizar que os resultados decorrem de uma implementação experimental utilizando o mecanismo de consenso PoW em uma rede privada com cinco mineradores. A literatura técnica contemporânea sugere que implementações otimizadas do Ethereum, especialmente aquelas que incorporam mecanismos como PoS ou variantes de consenso bizantino, podem apresentar desempenhos substancialmente superiores.

A investigação corrobora a complexidade inerente à análise de desempenho em redes *blockchain*, destacando a importância de abordagens metodológicas rigorosas para compreensão dos padrões de processamento transacional.

### 5.2.4 Discussão das Implicações Tecnológicas

Os resultados experimentais obtidos para a rede Ethereum evidenciam características operacionais que possuem implicações significativas para aplicações práticas desta tecnologia. O tempo médio de convergência de blocos relativamente elevado (149,91 segundos na média global) limita a aplicabilidade da plataforma em cenários que exigem confirmações transacionais rápidas, como sistemas de pagamento em tempo real ou aplicações interativas.

Por outro lado, a estabilidade relativa observada no comportamento dos mineradores, evidenciada pela diferença moderada entre os tempos médios de extração (17,63 segundos entre o melhor e o pior desempenho), sugere uma distribuição razoavelmente equilibrada da capacidade de processamento, característica desejável em sistemas descentralizados.

A forte correlação identificada entre latência de rede e tempo de extração (coeficiente de Pearson de 0,72) ressalta a importância crítica da infraestrutura de comunicação para o

desempenho global do sistema. Esta observação sugere que a otimização da topologia de rede e dos protocolos de comunicação poderia resultar em melhorias significativas no desempenho, sem necessidade de modificações fundamentais no mecanismo de consenso ou na arquitetura da plataforma.

A variabilidade significativa nos valores extremos de tempo de extração, particularmente evidente no Minerador 5 (amplitude de 720,10 s), indica potenciais instabilidades operacionais que poderiam comprometer a confiabilidade do sistema em aplicações críticas. A identificação e mitigação dos fatores que contribuem para esta variabilidade constituem aspectos relevantes para o aprimoramento da robustez operacional da plataforma.

## 5.3 Resultados na Rede Cosmos

### 5.3.1 Análise do Tempo de Processamento de Blocos

A análise do tempo de processamento de blocos na rede Cosmos revela características operacionais distintivas desta plataforma, fundamentada no mecanismo de consenso Tendermint BFT (Byzantine Fault Tolerance). Os experimentos realizados possibilitaram a quantificação deste parâmetro crítico, conforme apresentado na tabela 5.5.

| Validador | Tempo Médio de Processamento (s) |
|---|---|
| Validador 1 | 3,91 |
| Validador 2 | 4,76 |
| Validador 3 | 4,83 |
| Validador 4 | 4,78 |
| Validador 5 | 4,82 |

Tabela 5.5 – Distribuição do tempo médio de processamento de blocos por validador na rede Cosmos

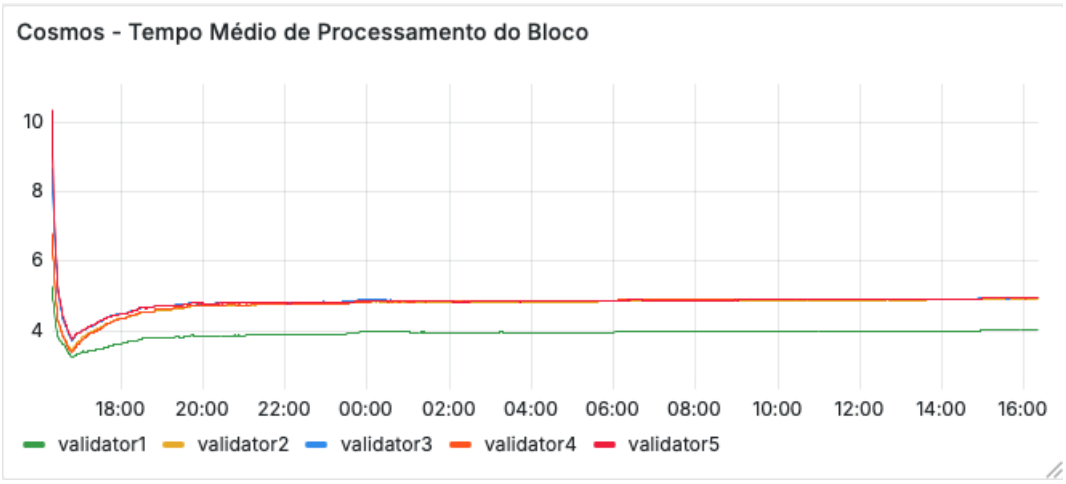


Figura 5.3 – Representação gráfica do tempo médio de processamento do bloco

A análise estatística dos dados experimentais revela um tempo médio global de processamento de 4,62 segundos, significativamente inferior aos valores observados na rede Ethereum. Esta eficiência operacional superior pode ser atribuída primariamente ao mecanismo de consenso Tendermint BFT, que elimina a necessidade de resolução de problemas criptográficos complexos, característicos dos sistemas baseados em PoW.

Um aspecto notável dos resultados obtidos é a homogeneidade observada entre os validadores 2 a 5, com variação inferior a 0,1 segundo nos tempos médios de processamento. Esta uniformidade operacional constitui uma característica desejável em sistemas distribuídos, contribuindo para a previsibilidade e confiabilidade do comportamento global da rede.

O Validador 1 apresentou desempenho significativamente superior aos demais, com tempo médio de processamento de 3,91 segundos, representando uma redução de aproximadamente 18,8% em relação ao valor mais elevado de 4,83 s, que pertence ao Validador 3. Esta divergência sugere a existência de otimizações específicas na configuração ou operação deste validador, que poderiam potencialmente ser estendidas aos demais nós para aprimoramento global do sistema.

### 5.3.2 Análise da Latência de Rede

A latência de rede constitui um fator determinante para a eficiência operacional de sistemas distribuídos, particularmente relevante em mecanismos de consenso bizantino como o Tendermint, que dependem de comunicação intensiva entre os nós validadores. A mensuração experimental deste parâmetro na rede Cosmos implementada resultou nos valores apresentados na Tabela 5.6.

| **Validador** | **Latência Média (ms)** |
|---|---|
| Validador 1 | 10,50 |
| Validador 2 | 10,70 |
| Validador 3 | 10,70 |
| Validador 4 | 10,70 |
| Validador 5 | 10,70 |

Tabela 5.6 – Distribuição da latência média por validador na rede Cosmos

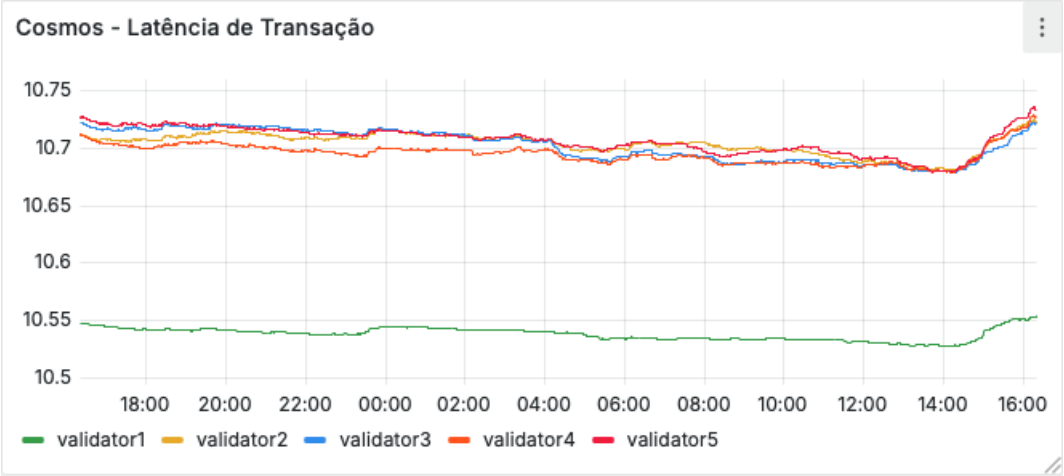


Figura 5.4 – Representação gráfica da latência de rede

A análise dos dados experimentais revela valores de latência notavelmente baixos e consistentes entre os validadores, com média global de 10,66 ms. Esta uniformidade na latência, particularmente evidente entre os Validadores 2 a 5, que apresentam valores idênticos de 10,70 ms, contribui significativamente para a estabilidade operacional da rede e para a previsibilidade do comportamento do sistema.

O Validador 1 apresentou latência ligeiramente inferior em relação aos demais, corroborando a hipótese de otimizações específicas em sua configuração, conforme sugerido pela análise do tempo de processamento. No entanto, a diferença absoluta relativamente pequena de 0,20 ms, sugere que este fator isolado não explica integralmente a superioridade operacional deste validador, indicando a provável existência de outros fatores otimizados em sua configuração.

A correlação entre os valores de latência e os tempos de processamento não se mostrou estatisticamente significativa no contexto da rede Cosmos, contrariamente ao observado na rede Ethereum. Esta divergência pode ser atribuída à magnitude absoluta significativamente menor dos valores de latência na rede Cosmos, reduzindo seu impacto proporcional no desempenho global do sistema.

### 5.3.3 Análise do Throughput Transacional

O *throughput* transacional, representando a capacidade de processamento da rede em termos do número de transações processadas por unidade de tempo, foi mensurado experimentalmente para cada validador da rede Cosmos, conforme apresentado na tabela 5.7.

| Validador | Throughput (TPS) |
|---|---|
| Validador 1 | 0,0268 |
| Validador 2 | 0,0265 |
| Validador 3 | 0,0269 |
| Validador 4 | 0,0271 |
| Validador 5 | 0,0271 |

Tabela 5.7 – Distribuição do throughput transacional por validador na rede cosmos

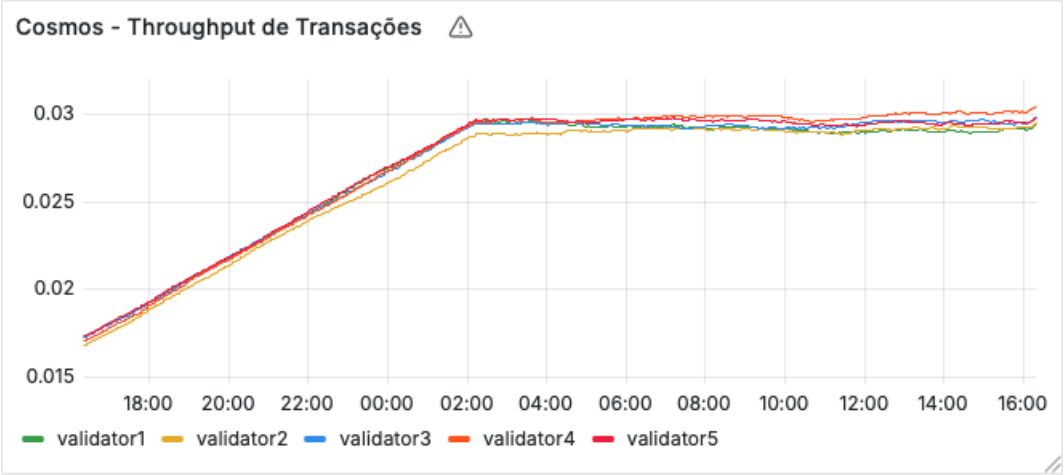


Figura 5.5 – Representação gráfica do throughput transacional

A análise estatística dos dados experimentais revela um *throughput* médio global de 0,027 TPS, valor que, embora aparentemente modesto, deve ser interpretado no contexto específico da implementação experimental. É fundamental ressaltar que este valor não representa uma limitação intrínseca da tecnologia Cosmos, mas sim uma consequência das características específicas do ambiente de teste e do volume controlado de transações submetidas durante o período experimental.

A literatura especializada e documentações técnicas da plataforma Cosmos reportam capacidades de *throughput* significativamente superiores em ambientes de produção otimizados, com valores típicos entre 5.000 e 10.000 TPS sob condições ideais. A discrepância em relação ao valor experimentalmente observado pode ser atribuída a diversos fatores, incluindo limitações deliberadas na configuração experimental, ausência de otimizações específicas para alta performance e, principalmente, o volume reduzido de transações submetidas ao sistema durante o período de análise.

Um aspecto notável dos resultados obtidos é a uniformidade dos valores de *throughput* entre os validadores, com variação máxima de aproximadamente 2,2% (entre 0,0265 e 0,0271 TPS). Esta homogeneidade sugere um balanceamento efetivo da carga transacional entre os nós validadores, característica desejável em sistemas distribuídos que visa evitar gargalos operacionais.

### 5.3.4 Análise da Capacidade de Processamento por Bloco

Uma métrica particularmente relevante para a avaliação da eficiência operacional e do potencial de escalabilidade da rede Cosmos é o número médio de transações processadas por bloco. Os experimentos realizados possibilitaram a quantificação deste parâmetro, conforme apresentado na tabela 5.8.

| **Validador** | **Transações por Bloco (média)** |
|---|---|
| Validador 1 | 2.317 |
| Validador 2 | 2.291 |
| Validador 3 | 2.326 |
| Validador 4 | 2.344 |
| Validador 5 | 2.338 |

Tabela 5.8 – Distribuição do número médio de transações por bloco na rede Cosmos

A análise dos dados experimentais revela um número médio global de 2.323 transações por bloco, valor significativamente elevado que demonstra a capacidade da plataforma Cosmos de processar eficientemente lotes volumosos de transações em cada ciclo de consenso. Esta característica é particularmente relevante para o potencial de escalabilidade da plataforma, uma vez que permite acomodar picos transacionais sem deterioração significativa do desempenho.

A homogeneidade observada entre os validadores, com variação máxima de aproximadamente 2,3% no número médio de transações por bloco, corrobora a hipótese de balanceamento efetivo da carga operacional entre os nós, contribuindo para a estabilidade global do sistema.

A combinação de um número elevado de transações por bloco com um tempo de processamento relativamente baixo resulta em um potencial de *throughput* teórico significativamente superior ao valor experimentalmente observado. Esta discrepância sugere que, sob condições de carga transacional mais intensa e com otimizações específicas, a plataforma poderia operar com eficiência significativamente superior à observada no presente experimento.

### 5.3.5 Discussão das Implicações Tecnológicas

Os resultados experimentais obtidos para a rede Cosmos evidenciam características operacionais que possuem implicações significativas para aplicações práticas desta tecnologia. O tempo médio de processamento de blocos relativamente baixo (4,62 segundos na média global) viabiliza a aplicabilidade da plataforma em cenários que exigem confirmações transacionais rápidas, como sistemas de pagamento em tempo real ou aplicações interativas.

A homogeneidade operacional observada entre os validadores, evidenciada pela variação limitada nos tempos médios de processamento e nos valores de latência, contribui para a previsibilidade e confiabilidade do comportamento global do sistema. Esta característica é parti-

cularmente relevante para aplicações críticas que requerem garantias robustas de desempenho e disponibilidade.

O elevado número médio de transações por bloco (2.323) demonstra a capacidade da plataforma de processar eficientemente lotes volumosos de operações, característica essencial para cenários de alta demanda transacional. Combinado com o tempo relativamente baixo de processamento, este parâmetro sugere um potencial significativo de escalabilidade, particularmente relevante para aplicações empresariais ou casos de uso que envolvam volumes elevados de transações.

A uniformidade nos valores de latência entre os validadores (com exceção da ligeira redução observada no Validador 1) sugere uma configuração de rede bem otimizada, minimizando a ocorrência de gargalos comunicacionais que poderiam comprometer o desempenho global do sistema. Esta característica contribui para a robustez operacional da plataforma, particularmente relevante em mecanismos de consenso bizantino, que dependem fundamentalmente de comunicação eficiente entre os nós validadores.

## 5.4 Análise Comparativa entre Ethereum e Cosmos

A partir dos resultados experimentais obtidos, é possível estabelecer uma análise comparativa sistemática entre as redes Ethereum e Cosmos, fundamentada em parâmetros objetivos de desempenho e características operacionais. Esta comparação visa identificar as especificidades de cada plataforma e suas implicações para diferentes cenários de aplicação.

### 5.4.1 Análise Comparativa do Tempo de Processamento

O tempo médio de processamento de blocos constitui um dos parâmetros mais distintivos entre as plataformas analisadas, conforme evidenciado na tabela 5.9.

| **Plataforma** | **Tempo Médio (s)** | **Tempo Mínimo (s)** | **Tempo Máximo (s)** |
|---|---|---|---|
| Ethereum | 149,91 | 25,90 | 746,00 |
| Cosmos | 4,62 | 3,91 | 4,83 |

Tabela 5.9 – Análise comparativa do tempo de processamento entre Ethereum e Cosmos

A diferença observada no tempo médio de processamento representa um fator de aproximadamente 32,4 vezes, evidenciando a superioridade significativa da plataforma Cosmos neste parâmetro específico. Esta disparidade pode ser atribuída primariamente aos mecanismos de consenso fundamentalmente distintos utilizados pelas plataformas: o PoW do Ethereum, que requer a resolução de problemas criptográficos computacionalmente intensivos, contra o Tendermint BFT do Cosmos, que utiliza um processo de votação determinístico entre validadores pré-definidos.

Além da diferença na magnitude absoluta dos tempos médios, destaca-se a variabilidade significativamente menor observada na plataforma Cosmos. Enquanto o Ethereum apresentou uma amplitude de 720,10 segundos entre os tempos mínimo e máximo, o Cosmos demonstrou uma variação de apenas 0,92 segundos, representando um fator aproximado de, 782 vezes em termos de estabilidade temporal. Esta característica tem implicações significativas para a previsibilidade operacional e para a consistência da experiência de usuário em aplicações críticas.

### 5.4.2 Análise Comparativa da Latência de Rede

A latência de rede constitui um parâmetro crítico para sistemas distribuídos, impactando diretamente a eficiência da comunicação entre os nós e, consequentemente, o desempenho global do sistema. A comparação deste parâmetro entre as plataformas analisadas está sistematizada na tabela 5.10.

| **Plataforma** | **Latência Média (ms)** | **Variação Internodal (ms)** |
|---|---|---|
| Ethereum | 162,86 | 249,66 (108,45 a 358,10) |
| Cosmos | 10,66 | 0,20 (10,50 a 10,70) |

Tabela 5.10 – Análise comparativa da latência de rede entre Ethereum e Cosmos

A diferença observada na latência média representa um fator de aproximadamente 15,3 vezes, evidenciando a superioridade significativa da infraestrutura de rede da plataforma Cosmos neste parâmetro específico. Esta disparidade pode ser atribuída a múltiplos fatores, incluindo potenciais diferenças na topologia de rede, nos protocolos de comunicação e, possivelmente, na localização geográfica dos nós.

Particularmente notável é a diferença na variabilidade da latência entre os nós. Enquanto a rede Ethereum apresentou uma variação de 249,66 ms entre os valores mínimo e máximo, a rede Cosmos demonstrou uma variação de apenas 0,20 ms, representando um fator aproximado de 1.248 vezes em termos de uniformidade comunicacional. Esta homogeneidade na latência da rede Cosmos contribui significativamente para a previsibilidade operacional do sistema e para a estabilidade do processo de consenso.

A correlação entre latência e tempo de processamento mostrou-se estatisticamente significativa na rede Ethereum (coeficiente de Pearson de 0,72), mas não apresentou significância estatística na rede Cosmos. Esta divergência pode ser atribuída à magnitude absoluta significativamente menor dos valores de latência na rede Cosmos, reduzindo seu impacto proporcional no desempenho global do sistema, bem como à natureza fundamentalmente distinta dos mecanismos de consenso empregados.

### 5.4.3 Análise Comparativa do Throughput Transacional

O *throughput* transacional representa a capacidade efetiva de processamento das redes em termos do número de transações confirmadas por unidade de tempo. A comparação deste parâmetro entre as plataformas analisadas está apresentada na tabela 5.11.

| **Plataforma** | **Throughput Médio (TPS)** |
|---|---|
| Ethereum | 0,14 |
| Cosmos | 0,03 |

Tabela 5.11 – Análise comparativa do throughput transacional entre ethereum e cosmos

Contrariamente às tendências observadas nos parâmetros anteriores, o *throughput* médio observado experimentalmente foi superior na rede Ethereum em comparação com a rede Cosmos, representando um fator de aproximadamente 4,7 vezes. No entanto, esta aparente superioridade deve ser interpretada com cautela no contexto das condições experimentais específicas.

É fundamental ressaltar que o *throughput* observado não representa necessariamente a capacidade máxima teórica das plataformas, mas sim o volume efetivo de transações processadas durante o período experimental, que pode ter sido influenciado por diversos fatores além das características intrínsecas das tecnologias, incluindo o volume de transações submetidas e características específicas da carga transacional.

Um aspecto particularmente relevante para a interpretação destes resultados é a relação entre o *throughput* e o tempo de processamento. No caso da rede Cosmos, que apresentou tempo médio de processamento significativamente inferior, o *throughput* relativamente baixo não pode ser atribuído a limitação de processamento, mas provavelmente ao volume reduzido de transações submetidas durante o experimento.

Esta hipótese é corroborada pelo elevado número médio de transações por bloco observado na rede Cosmos (2.323), que, combinado com o tempo médio de processamento, resultaria em um *throughput* teórico significativamente superior ao observado experimentalmente, na ordem de aproximadamente 502,8 TPS. A discrepância em relação ao valor experimentalmente observado de 0,03 TPS, sugere que a rede estava operando significativamente abaixo de sua capacidade máxima de processamento durante o período experimental.

### 5.4.4 Análise da Variabilidade do Desempenho

A variabilidade do desempenho constitui um parâmetro relevante para a previsibilidade operacional e para a confiabilidade de sistemas distribuídos. A análise comparativa deste parâmetro entre as plataformas estudadas revela padrões distintivos que têm implicações significativas para diferentes cenários de aplicação.

Na rede Ethereum, a variação no tempo médio de processamento entre o melhor e o pior desempenho dos mineradores foi de 17,63 segundos, representando aproximadamente 12,4% do valor médio global. Em contraste, na rede Cosmos, esta variação foi de 0,92 segundos, representando aproximadamente 19,9% do valor médio global. Em termos percentuais, portanto, as duas plataformas apresentam variabilidades moderadas e relativamente próximas.

No entanto, a análise dos casos extremos revela diferenças muito mais significativas. Na rede Ethereum, a razão entre o pior e o melhor tempo observado foi de aproximadamente 28,8, evidenciando uma amplitude extrema nos valores. Na rede Cosmos, esta razão foi de apenas 1,2 , demonstrando uma estabilidade operacional significativamente superior.

Esta estabilidade superior da rede Cosmos pode ser atribuída a múltiplos fatores, incluindo o mecanismo de consenso determinístico Tendermint BFT, a homogeneidade da latência de rede e, possivelmente, uma maior uniformidade na configuração e capacidade dos nós validadores.

### 5.4.5 Análise das Implicações para Aplicações Práticas

As características operacionais distintivas das plataformas analisadas têm implicações significativas para sua adequação a diferentes cenários de aplicação. A partir dos resultados experimentais, é possível delinear domínios de aplicação preferenciais para cada tecnologia:

- **Ethereum (PoW):** As características operacionais observadas na rede Ethereum, incluindo tempo de processamento relativamente elevado e variabilidade significativa no desempenho, sugerem maior adequação a aplicações que priorizam descentralização e segurança em detrimento da velocidade de confirmação transacional. Exemplos incluem:
  - *Contratos financeiros complexos* que requerem elevado nível de segurança e imutabilidade, onde a velocidade de processamento não constitui fator crítico.
  - *Sistemas de registro imutável* para documentos, ativos digitais ou direitos de propriedade, onde a finalidade probabilística robusta do PoW proporciona garantias adequadas contra modificações não autorizadas.
  - *Aplicações que exigem elevado grau de descentralização*, beneficiando-se da natureza aberta e resistente a censura do mecanismo de consenso PoW, potencialmente com milhares de mineradores independentes.
- **Cosmos (Tendermint BFT):** As características operacionais observadas na rede Cosmos, incluindo tempo de processamento relativamente baixo e estabilidade superior, sugerem maior adequação a aplicações que requerem confirmações rápidas e comportamento previsível. Exemplos incluem:

- Sistemas de pagamento que exigem confirmações rápidas e garantias robustas de finalidade, proporcionando experiência de usuário comparável a sistemas de pagamento centralizados convencionais.
- Plataformas de interoperabilidade entre diferentes *blockchains*, facilitando a transferência eficiente de ativos e informações entre múltiplos ecossistemas.
- Aplicações empresariais que requerem elevado *throughput*, baixa latência e garantias robustas de finalidade, como sistemas de rastreamento de cadeia de suprimentos ou plataformas de negociação de ativos.

É fundamental ressaltar que estas recomendações baseiam-se nas características específicas das implementações analisadas experimentalmente, e que ambas as plataformas possuem flexibilidade significativa para adaptação a diferentes requisitos através de modificações em suas configurações ou arquiteturas.

### 5.4.6 Síntese Comparativa

A análise experimental comparativa entre as redes Ethereum e Cosmos possibilita a identificação das características fundamentais que distinguem estas plataformas, conforme sintetizado na tabela 5.12.

| **Característica** | **Ethereum (PoW)** | **Cosmos (Tendermint BFT)** |
|---|---|---|
| Tempo de processamento | Elevado (149,91s em média) com variabilidade significativa | Reduzido (4,62s em média) com elevada consistência |
| Latência de rede | Elevada (162,86ms) com variação significativa entre mineradores | Reduzida (10,66ms) com variação mínima entre validadores |
| Estabilidade operacional | Previsibilidade moderada com variação significativa nos valores extremos | Elevada previsibilidade com comportamento operacional uniforme |
| Finalidade transacional | Probabilística, aumentando progressivamente com o número de confirmações subsequentes | Determinística, com garantia absoluta de imutabilidade após obtenção do consenso |
| Potencial de escalabilidade | Limitado intrinsecamente pelo mecanismo de consenso PoW, que impõe sobrecarga computacional crescente | Elevado, conforme evidenciado pela capacidade de processamento eficiente de lotes volumosos de transações |

Tabela 5.12 – Síntese comparativa das características fundamentais de Ethereum e Cosmos

## 5.5 Conclusões e Perspectivas

Os experimentos realizados neste trabalho destacaram as diferenças substanciais entre as plataformas Ethereum e Cosmos em relação a parâmetros críticos como desempenho, estabilidade operacional e potencial de escalabilidade. Os resultados obtidos reforçam as características intrínsecas de cada plataforma, decorrentes dos mecanismos de consenso adotados (PoW no Ethereum e Tendermint BFT no Cosmos).

A rede Ethereum apresentou tempos médios de processamento significativamente mais elevados, aliados a uma maior variabilidade operacional. Essa característica ressalta uma limitação natural do mecanismo de consenso PoW em aplicações que exigem confirmações rápidas e previsibilidade consistente. No entanto, a forte correlação identificada entre latência de rede e desempenho operacional evidencia que melhorias na infraestrutura de comunicação poderiam amenizar algumas dessas limitações, possibilitando melhor desempenho sem alterar o consenso fundamental.

Por outro lado, a rede Cosmos demonstrou um desempenho superior, com baixos tempos de processamento e alta estabilidade operacional. Essas vantagens são diretamente atribuídas ao mecanismo determinístico de consenso Tendermint BFT, que elimina a necessidade de operações criptográficas computacionalmente intensivas, garantindo rapidez e previsibilidade. A capacidade de processar inúmeras transações por bloco sugere ainda um significativo potencial de escalabilidade, especialmente relevante para aplicações corporativas ou sistemas de alto volume transacional.

Diante dos resultados, é recomendável que a escolha entre Ethereum e Cosmos seja fundamentada nas exigências específicas da aplicação, considerando fatores como segurança, velocidade, descentralização e previsibilidade operacional. Aplicações que demandam um alto grau de descentralização e resistência à censura continuarão encontrando vantagens na robustez do Ethereum. Já aplicações que priorizam eficiência operacional, rapidez nas transações e consistência previsível terão melhores resultados com a plataforma Cosmos.

Considerando o rápido desenvolvimento e evolução das tecnologias *blockchain*, futuras pesquisas devem acompanhar as atualizações significativas, como a migração do Ethereum para PoS e os avanços no ecossistema interoperável do Cosmos. Esses estudos adicionais contribuirão para determinar se as diferenças observadas neste trabalho permanecerão relevantes, ou se haverá uma convergência gradual das plataformas para padrões mais semelhantes de desempenho e aplicação prática.

# 6 Considerações Finais

## 6.1 Conclusão

Este estudo abordou a implementação e análise comparativa das plataformas Ethereum e Cosmos, com foco em aplicações na indústria 4.0. Foi proposta uma arquitetura baseada na plataforma Cosmos, destacando especialmente a integração com um banco de dados PostgreSQL para otimizar a indexação, consulta e monitoramento dos dados provenientes da *blockchain*.

Os resultados experimentais demonstraram que a rede Ethereum oferece características importantes, especialmente no que diz respeito à segurança robusta, descentralização e estabilidade na distribuição de carga. Contudo, apresentou limitações notáveis relacionadas ao tempo elevado de processamento de blocos e alta variabilidade operacional, aspectos que restringem seu uso em contextos industriais que exigem alta velocidade e previsibilidade nas transações.

Por outro lado, a plataforma Cosmos revelou-se superior em desempenho operacional, com tempos de processamento significativamente menores e maior estabilidade no comportamento dos validadores. Essas características, derivadas do consenso Tendermint BFT, mostram potencial considerável para aplicações industriais que exigem confirmação rápida e previsível das transações, além de escalabilidade eficiente sob demanda.

Adicionalmente, a integração da rede Cosmos com um sistema relacional PostgreSQL permitiu uma extração eficiente e automatizada dos dados, proporcionando recursos avançados como dashboards dinâmicos para monitoramento em tempo real. Este modelo híbrido une a imutabilidade e rastreabilidade inerentes à tecnologia *blockchain* com a eficácia e rapidez de consultas estruturadas típicas de bancos de dados tradicionais, estabelecendo-se como uma solução robusta para atender às demandas específicas da indústria 4.0.

## 6.2 Reflexões sobre Blockchain e Indústria 4.0

A integração entre *blockchain* e indústria 4.0 marca uma mudança importante nos processos industriais, especialmente em termos de segurança, transparência e automação. Este estudo evidenciou que estas tecnologias combinadas são capazes de solucionar desafios fundamentais, como proteção e integridade dos dados, rastreabilidade eficiente e automação segura de operações industriais.

A capacidade da tecnologia *blockchain* em garantir proteção reforçada contra adulterações e ataques cibernéticos se mostra vital para ambientes industriais altamente conectados e autônomos. Além disso, a aplicação desta tecnologia para a rastreabilidade em cadeias produtivas possibilita não apenas maior transparência, mas facilita a rápida identificação e mitigação de

fraudes ou erros operacionais, contribuindo para um melhor controle regulatório e eficiência operacional.

A automação industrial através de contratos inteligentes ainda agrega eficiência operacional, permitindo operações diretas e seguras entre máquinas e sistemas, reduzindo significativamente a necessidade de intermediários e aumentando a confiança nas transações.

Dessa forma, a união da tecnologia *blockchain* com os processos industriais modernos apresenta-se como um avanço estratégico, essencial para enfrentar os desafios impostos pela transformação digital na indústria.

## 6.3 Contribuições do Trabalho

Este trabalho proporcionou um avanço na compreensão prática sobre os desafios e as potencialidades do uso da *blockchain* na indústria 4.0, especialmente por meio da implementação experimental das redes Ethereum e Cosmos. A pesquisa permitiu avaliar objetivamente os benefícios e limitações concretas dessas plataformas em cenários industriais típicos.

Uma das principais contribuições foi demonstrar claramente como a *blockchain*, combinada a contratos inteligentes, pode garantir a segurança e imutabilidade das informações industriais, além de permitir uma integração eficaz com sistemas tradicionais, como bancos de dados relacionais. O modelo híbrido proposto mostrou-se promissor para cenários que requerem tanto a segurança da descentralização quanto a eficiência operacional.

Este estudo também abre espaço para novas investigações voltadas a melhorias na escalabilidade e eficiência na recuperação e consulta de grandes volumes de dados da *blockchain*. A utilização futura de técnicas avançadas de indexação e pesquisa estruturada representa uma importante perspectiva para aprimorar ainda mais o desempenho dessas plataformas em contextos industriais complexos.

Em suma, este trabalho reafirma o potencial transformador da *blockchain* para o setor industrial, reforçando a importância desta tecnologia na melhoria contínua da segurança, transparência e eficácia das operações industriais cada vez mais interconectadas e automatizadas.

# Referências


AHAKONYE, L. A. C.; NWAKANMA, C. I.; KIM, D.-S. Tides of blockchain in iot cybersecurity. *Sensors*, MDPI, v. 24, n. 10, p. 3111, 2024.

Altoros. *Boeing Improves Operations with Blockchain and the Internet of Things*. 2024. Disponível em: <https://www.altoros.com/blog/boeing-improves-operations-with-blockchain-and-the-internet-of-things/>.

Amazon Web Services. *Blockchain for Supply Chain*. 2024. Disponível em: <https://aws.amazon.com/pt/blockchain/>.

AMOUSSOU-GUENOU, Y.; POZZO, A. D.; POTOP-BUTUCARU, M.; TUCCI-PIERGIOVANNI, S. Correctness of tendermint-core blockchains. In: SCHLOSS DAGSTUHL-LEIBNIZ-ZENTRUM FUER INFORMATIK. *22nd International Conference on Principles of Distributed Systems (OPODIS 2018)*. [S.l.], 2018.

ASIF, R.; HASSAN, S. R. Shaping the future of ethereum: Exploring energy consumption in proof-of-work and proof-of-stake consensus. *Frontiers in Blockchain*, Frontiers Media SA, v. 6, p. 1151724, 2023.

AUMASSON, J.-P.; KOLEGOV, D.; STATHOPOULOU, E. *Security Review of Ethereum Beacon Clients*. 2021. Disponível em: <https://arxiv.org/abs/2109.11677>.

BELTRANDO, L.; POTOP-BUTUCARU, M.; ALFARO, J. Tendertee: Secure tendermint. *Cryptology ePrint Archive*, 2022.

BEN-SASSON, E.; CHIESA, A.; GENKIN, D.; GORBUNOV, S.; ISHAI, Y.; RIABZEV, M.; SPOONER, N.; TROMER, E.; VIRZA, M. Snarks for C: Verifying program executions succinctly and in zero knowledge. In: *Advances in Cryptology - CRYPTO 2014*. Springer, 2014. p. 90–108. Disponível em: <https://eprint.iacr.org/2013/507.pdf>.

BENET, J. Ipfs-content addressed, versioned, p2p file system. *arXiv preprint arXiv:1407.3561*, 2014.

BENTOV, I.; LEE, C.-T.; MIZRAHI, A.; ROSENFELD, M. Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract]y. *SIGMETRICS Perform. Evaluation Rev.*, v. 42, p. 34–37, 2014. Disponível em: <https://api.semanticscholar.org/CorpusID:7263421>.

BHUDIA, A.; CARTWRIGHT, A.; CARTWRIGHT, E.; HURLEY-SMITH, D.; HERNANDEZ-CASTRO, J. Game theoretic modelling of a ransom and extortion attack on ethereum validators. *Proceedings of the 18th International Conference on Availability, Reliability and Security*, 2023.

BODKHE, U.; TANWAR, S.; PAREKH, K.; KHANPARA, P.; TYAGI, S.; KUMAR, N.; ALAZAB, M. Blockchain for industry 4.0: A comprehensive review. *Ieee Access*, IEEE, v. 8, p. 79764–79800, 2020.

BONEH, D.; DRIJVERS, M.; NEVEN, G. Compact multi-signatures for smaller blockchains. In: SPRINGER. *International Conference on the Theory and Application of Cryptology and Information Security*. [S.l.], 2018. p. 435–464.

BOSCHI, A.; POLLICE, F.; BATOCCHIO, A. Blockchain como elemento viabilizador na gestão da economia circular das cadeias de suprimentos. *ReserchGate*, 2020.

BUTERIN, V. et al. A next-generation smart contract and decentralized application platform. *white paper*, v. 3, n. 37, p. 2–1, 2014.

CARVALHO, M. de. *Construindo o saber: técnicas de metodologia científica*. [S.l.]: Papirus Editora, 1989. ISBN 9788530800710.

CHAUHAN, A.; MALVIYA, O. P.; VERMA, M.; MOR, T. S. Blockchain and scalability. In: IEEE. *2018 IEEE international conference on software quality, reliability and security companion (QRS-C)*. [S.l.], 2018. p. 122–128.

CHERVINSKI, J. O.; KREUTZ, D.; XU, X.; YU, J. Analyzing the performance of the inter-blockchain communication protocol. In: IEEE. *2023 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. [S.l.], 2023. p. 151–164.

CORTES-GOICOECHEA, M.; MOHANDAS-DARYANANI, T.; MUÑOZ-TAPIA, J. L.; BAUTISTA-GOMEZ, L. Can we run our ethereum nodes at home? *IEEE access*, IEEE, 2024.

DECKER, C.; WATTENHOFER, R. Information propagation in the bitcoin network. In: *IEEE P2P 2013 Proceedings*. [S.l.: s.n.], 2013. p. 1–10.

EL-DIN, M. N.; MARTINS, J. P.; RAMOS, N. M. M.; PEREIRA, P. F. The role of blockchain-secured digital twins in promoting smart energy performance-based contracts for buildings. *Energies*, v. 17, n. 14, 2024. ISSN 1996-1073. Disponível em: <https://www.mdpi.com/1996-1073/17/14/3392>.

ESSAID, M.; KIM, J.; JU, H. Inter-blockchain communication message relay time measurement and analysis in cosmos. *Applied Sciences*, MDPI, v. 13, n. 20, p. 11135, 2023.

Ethereum Foundation. *Geth: Go-Ethereum*. 2015. <https://geth.ethereum.org/>. Accessed: 2024-10-10.

European Parliament and Council of the European Union. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. 2016. Accessed: 2024-10-10. Disponível em: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.

FOUNDATION, E. *Ethereum 2.0: A Secure and Scalable Blockchain*. 2023. Disponível em: <https://ethereum.org/en/ethereum-2/>.

FOUNDATION, E. *ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER*. 2024. Disponível em: <https://ethereum.org/en/eth2/>.

GAI, K.; QIU, M.; SUN, X. A survey on fintech. *Journal of Network and Computer Applications*, v. 103, 10 2017.

GARCÍA, C. G.; VALDÉZ, E. R. N.; DÍAZ, V. G.; GARCÍA-BUSTELO, B. C. P.; LOVELLE, J. M. C. et al. A review of artificial intelligence in the internet of things. *International Journal Of Interactive Multimedia And Artificial Intelligence, 5*, 2019.

GARROCHO, C. T. B. Blockchain é tudo que você precisa: a integração e comunicação descentralizada dos sistemas da indústria 4.0. 2022.

GEBHARDT, A. Understanding additive manufacturing. Hanser publications Munich, Germany:, 2011.

GeeksforGeeks. *Blockchain Structure*. 2024. Disponível em: <https://www.geeksforgeeks.org/blockchain-structure/>.

GeeksforGeeks. *How does the Blockchain Work?* 2024. Disponível em: <https://www.geeksforgeeks.org/how-does-the-blockchain-work/>.

GOES, C. The interblockchain communication protocol: An overview. *arXiv preprint arXiv:2006.15918*, 2020.

GREENE, R.; JOHNSTONE, M. N. An investigation into a denial of service attack on an ethereum network. Security Research Institute, Edith Cowan University, 2018.

HASHEM, I.; YAQOOB, I.; ANUAR, N.; MOKHTAR, S.; GANI, A.; KHAN, S. The rise of "big data" on cloud computing: Review and open research issues. *Information Systems*, v. 47, p. 98–115, 07 2014.

HOSSAIN, M. T.; BADSHA, S.; SHEN, H. Porch: A novel consensus mechanism for blockchain-enabled future scada systems in smart grids and industry 4.0. In: IEEE. *2020 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*. [S.l.], 2020. p. 1–7.

Hub do Investidor. *Maximal Extractable Value (MEV)*. 2024. Disponível em: <https://hubdoinvestidor.com.br/maximal-extractable-value-mev/>.

IoTHub. *Combining IoT and Blockchain for Supply Chain Tracking*. 2024. Disponível em: <https://www.iothub.com.au/news/combining-iot-and-blockchain-for-supply-chain-tracking-492501>.

KANEVCHE, J.; KARAMACHOSKI, J.; PUNCHEVA, M.; MARINA, N. Trading application based on blockchain technology. *Tehnički glasnik*, Sveučilište Sjever, v. 15, n. 2, p. 282–286, 2021.

KASIREDDY, P. *How does Cosmos work? How does it compare to Bitcoin and Ethereum? (Part 2)*. 2020. Imagem. Disponível em: <https://www.preethikasireddy.com/post/how-does-cosmos-work-how-does-it-compare-to-bitcoin-and-ethereum-part-2>.

KHAN, P. W.; BYUN, Y.-C.; PARK, N. Iot-blockchain enabled optimized provenance system for food industry 4.0 using advanced deep learning. *Sensors*, v. 20, n. 10, 2020. ISSN 1424-8220. Disponível em: <https://www.mdpi.com/1424-8220/20/10/2990>.

KIAYIAS, A.; RUSSELL, A.; DAVID, B.; MICHEL, A. Ouroboros: A provably secure proof-of-stake blockchain protocol. *Annual International Cryptology Conference*, p. 357–388, 2017. Disponível em: <https://eprint.iacr.org/2016/889>.

KING, S.; NADAL, S. *PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake*. 2012. <https://peercoin.net/assets/paper/peercoin-paper.pdf>. Accessed: 2024-10-10.

KWON, J. Tendermint: Consensus without mining. *Draft v. 0.6, fall*, v. 1, n. 11, p. 1–11, 2014.

KWON, J.; BUCHMAN, E. A network of distributed ledgers. *Cosmos, dated*, p. 1–41, 2018.

LABS, P. *Prysmatic Labs Documentation*. 2021. Disponível em: <https://docs.prylabs.network/docs/getting-started>.

LAMPORT, L.; SHOSTAK, R.; PEASE, M. The byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, ACM, v. 4, n. 3, p. 382–401, 1982.

LARIMER, D. *Delegated Proof-of-Stake (DPoS)*. 2014. Bitshares Whitepaper. Disponível em: <https://bitshares.org/technology/delegated-proof-of-stake-consensus>.

LEE, I.; LEE, K. The internet of things (iot): Applications, investments, and challenges for enterprises. *Business Horizons*, v. 58, n. 4, p. 431–440, 2015. Disponível em: <https://EconPapers.repec.org/RePEc:eee:bushor:v:58:y:2015:i:4:p:431-440>.

Luo Zhu. *Ethereum: From PoW to PoS and Withdrawals in 2023*. 2024. Disponível em: <https://luozhu.io/2023/04/07/withdrawal.html>.

MEKNI, M.; LEMIEUX, A. Augmented reality : Applications , challenges and future trends. 2014. Disponível em: <https://api.semanticscholar.org/CorpusID:15436826>.

Metlabs. *Solidity, Smart Contracts, and Ethereum Virtual Machine (EVM)*. 2024. Disponível em: <https://metlabs.io/en/que-es-solidity-smart-contracts-blockchain-evm/>.

MILLER, A.; XIA, Y.; CROMAN, K.; SHI, E.; SONG, D. The honey badger of bft protocols. In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. New York, NY, USA: Association for Computing Machinery, 2016. (CCS '16), p. 31–42. ISBN 9781450341394. Disponível em: <https://doi.org/10.1145/2976749.2978399>.

MISHRA, B.; MOHANTA, P.; MAHANTY, B. Application of industry 4.0 in sustainability of servitized manufacturers. In: ____. [S.l.: s.n.], 2022. p. 38 – 60. ISBN 978-93-94318-00-7.

MOURTZIS, D.; ANGELOPOULOS, J.; PANOPOULOS, N. Blockchain integration in the era of industrial metaverse. *Applied Sciences*, MDPI, v. 13, n. 3, p. 1353, 2023.

NAKAMOTO, S. Bitcoin: A peer-to-peer electronic cash system. 2008.

Nilay Güler. *Network Architectures: Peer-to-Peer and Client-Server*. 2024. Disponível em: <https://medium.com/@gulernilay088/network-architectures-peer-to-peer-and-client-server-6fb3f0bf510c>.

Nucleo do Conhecimento. *Blockchain: Uma Introdução a Sua Tecnologia*. 2024. Disponível em: <https://www.nucleodoconhecimento.com.br/tecnologia/blockchain>.

ORLICKI, J. I. *Fair Proof-of-Stake using VDF+VRF Consensus*. 2020. Disponível em: <https://arxiv.org/abs/2008.10189>.

PAVLOFF, U.; AMOUSSOU-GUENOU, Y.; TUCCI-PIERGIOVANNI, S. Ethereum proof-of-stake under scrutiny. *Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing*, 2022.

PAVLYSHYN, I.; PETRENKO, A.; OPRYSHKO, B.; OLIINYK, B.; KAVUN, S. Social media impact on the 'cosmos' blockchain ecosystem: State and prospect. *Data Science Journal*, v. 23, n. 1, 2024.

PEASE, M.; SHOSTAK, R.; LAMPORT, L. Reaching agreement in the presence of faults. *Journal of the ACM (JACM)*, ACM New York, NY, USA, v. 27, n. 2, p. 228–234, 1980.

PLATT, M.; MCBURNEY, P. Sybil in the haystack: A comprehensive review of blockchain consensus mechanisms in search of strong sybil attack resistance. *Algorithms*, v. 16, p. 34, 2023.

RAMPAZZO, L. *Metodologia científica*. [S.l.]: Edições Loyola, 2005. ISBN 9788515024988.

SCHOEDON, A. *Discv5: The New Peer Discovery Protocol for Ethereum 2.0*. 2020. <https://github.com/ethereum/devp2p/blob/master/discv5/discv5.md>.

SIEGEL, D. *Understanding The DAO Attack*. 2016. <https://www.coindesk.com/understanding-dao-hack-journalists>. Accessed: 2024-10-10.

SketchBubble. *Proof of Work vs Proof of Stake*. 2024. Disponível em: <https://www.sketchbubble.com/en/presentation-proof-of-work-vs-proof-of-stake.html>.

SURMONT, J.; WANG, W.; CUTSEM, T. V. Static application security testing of consensus-critical code in the cosmos network. In: IEEE. *2023 5th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*. [S.l.], 2023. p. 1–8.

SZABO, N. Formalizing and securing relationships on public networks. *First Monday*, v. 2, 1997. Disponível em: <https://api.semanticscholar.org/CorpusID:33773111>.

TEAM, L. *LibP2P: A Modular Network Stack*. [S.l.], 2019. Disponível em: <https://libp2p.io/>.

TEISSERENC, B.; SEPASGOZAR, S. Adoption of blockchain technology through digital twins in the construction industry 4.0: A pestels approach. *Buildings*, MDPI, v. 11, n. 12, p. 670, 2021.

TYAGI, A. K.; DANANJAYAN, S.; AGARWAL, D.; AHMED, H. F. T. Blockchain—internet of things applications: Opportunities and challenges for industry 4.0 and society 5.0. *Sensors*, v. 23, n. 2, 2023. ISSN 1424-8220. Disponível em: <https://www.mdpi.com/1424-8220/23/2/947>.

UCBAS, Y.; ELEYAN, A.; HAMMOUDEH, M.; ALOHALY, M. Performance and scalability analysis of ethereum and hyperledger fabric. *IEEE Access*, IEEE, 2023.

Wolf Automation. *What does IO-Link mean in Smart Manufacturing?* 2024. Disponível em: <https://www.wolfautomation.com/blog/what-does-iolink-mean-in-smart-manufacturing/>.

WOOD, G. *Ethereum: A Secure Decentralised Generalised Transaction Ledger*. [S.l.], 2014. Disponível em: <https://ethereum.github.io/yellowpaper/paper.pdf>.

YETIS, H.; KARAKOSE, M.; BAYGIN, N. Blockchain-based mass customization framework using optimized production management for industry 4.0 applications. *Engineering Science and Technology, an International Journal*, v. 36, p. 101151, 2022. ISSN 2215-0986. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2215098622000593>.

ZHANG, M.; LI, R.; DUAN, S. Max attestation matters: Making honest parties lose their incentives in ethereum {PoS}. In: *33rd USENIX Security Symposium (USENIX Security 24)*. [S.l.: s.n.], 2024. p. 6255–6272.