Uso de Blockchain na Indústria 4.0: Uso do Hyperledger Fabric no projeto FASTEN

Carlos M. Pinto[1], Mattheus S. Santos[2], Rômulo L. A. S. Soares[2], José Maria N. David[2], Regina Braga[2], Mário Dantas[2]

[1]Departamento de Circuitos Elétricos - Faculdade de Engenharia Elétrica
Universidade Federal de Juiz de Fora (UFJF) – Juiz de Fora, MG – Brazil

[2]Departamento de Ciência da Computação
Universidade Federal de Juiz de Fora (UFJF) – Juiz de Fora, MG – Brazil

{mattheussantos, romulosoares, mario.dantas}@ice.ufjf.br

carlos.magnun@engenharia.ufjf.br

{jose.david, regina.braga}@ufjf.edu.br

Abstract. *In Industry 4.0, information security, especially in communication between machines in a production environment needs to be explored. Communication between IIoT (Industrial Internet of Thing) devices has a high vulnerability rate. The FASTEN project presents a communication solution between the devices. However, the lack of data security is still a challenge. This article presents a solution, based on blockchain concepts, to address information security in an industry environment, considering the FASTEN project, maintaining better communication between IIoT devices and users.*

Resumo. *Na Indústria 4.0, a segurança da informação, principalmente na comunicação entre máquinas do meio de produção necessita ser explorada. A comunicação entre dispositivos IIoT (Industrial Internet of Things), tem um alto índice de vulnerabilidade. Neste contexto, o projeto FASTEN apresenta uma solução de comunicação entre dispositivos. Porém, a falta de segurança dos dados ainda é um desafio. Este artigo apresenta uma solução, considerando os preceitos da tecnologia de blockchain, para tratar a segurança da informação no ambiente industrial, considerando o projeto FASTEN melhorando a segurança na comunicação entre os dispositivos IIoT.*

1. Introdução

Com a evolução e o desenvolvimento de tecnologias na área industrial, surgem novas preocupações em relação à segurança da informação. A incorporação de novas tecnologias nas fábricas, como sensores e dispositivos que possuem considerável capacidade de computação e comunicação, agilizou o processo de fabricação, mas trouxe novos desafios. Estes dispositivos e sensores, conhecidos como IIoT (*Industrial Internet of Things*) [Gilchrist 2016], possuem protocolos de comunicação vulneráveis, o que levanta uma questão de segurança referente a implantação desta tecnologia na indústria.

Neste contexto, foi desenvolvido o projeto H2020 FASTEN, em parceria com a UE-Brasil [Costa et al. 2020], que consiste em um *middleware* para a indústria 4.0, com

o intuito de garantir uma comunicação entre os dispositivos IIoT e os usuários. O projeto traz avanços na comunicação entre dispositivos de IIoT, mas precisa de um suporte para segurança dos dados. Nesse sentido, a abordagem apresentada neste artigo utiliza *blockchain*, mais especificamente o framework Hyperledger Fabric [Androulaki et al. 2018] e seus paradigmas de segurança, para apoiar a segurança na comunicação entre os dispositivos no contexto do projeto H2020 FASTEN [Rodrigues Pereira et al. 2018]. Essa vulnerabilidade de comunicação pode levar a disponibilização de informações estratégicas das empresas, o que compromete seu desempenho considerando, por exemplo, a concorrência.

Como contribuição, o artigo detalha o trabalho desenvolvido considerando a segurança nesse novo cenário da Indústria 4.0 de maneira geral e no projeto H2020 FASTEN de maneira específica. A proposta de solução foca na implementação de uma rede de *blockchain* para as validações e para requisições de segurança de dados, e tem como exemplo de uso o ambiente do FASTEN framework. O objetivo da solução é assegurar que somente quem possui devida autorização possa acessar e operar os dispositivos e informações que compõem o ambiente.

A partir de estudos em anteriores da tecnologia *blockchain* e principalmente o estudo do artigo Design and Implementation of an Integrated IoT Blockchain Platform for Sensing Data Integrity [Hang and Kim 2019] e sua aplicabilidade, que consiste num sistema de integração para plataformas de dispositivos IoT, utilizando a tecnologia de *blockchain*, utilizando de uma rede definida manualmente para o sistema de exemplo, trazendo escalabilidade, alta taxa de transferência, leveza e transparência, requisitos fundamentais para o iot devido a baixa capacidade de processamento e armazenamento de algum desses dispositivos, e o BlockFlow: Trust in Scientific Provenance Data [Coelho et al. 2019], que descreve a criação de uma arquitetura baseada em *blockchain* para gerir e armazenar uma rede de proveniência de dados para suporte em pesquisas científicas em um cenário colaborativo de forma automatizada. Ambos trabalham com uma plataforma descentralizada chamada Hyperledger Fabric, em versões anteriores a qual este artigo desenvolve.

Em nosso projeto desenvolvemos um sistema para gerenciamento e criação de uma rede de forma automatizada na versão 2.2.2 do hyperledger Fabric, onde nos baseamos nos estudos de ambos artigos para desenvolver uma plataforma de fácil uso para a criação da rede, trazendo os benefícios do *blockchain*, e com o objetivo de implementação e utilização por dispositivos IIoT presentes da Indústria 4.0, contexto abordado pelo projeto FASTEN.

O artigo está organizado em 5 seções. Na seção 2 são apresentados alguns conceitos relevantes para a proposta. Na seção 3 é discutida a solução e um exemplo de uso da rede na proposta no contexto do projeto FASTEN e exemplo de uso da rede no contexto do projeto FASTEN será apresentado e na seção 3 são apresentadas as considerações finais e trabalhos futuros e na seção 5 é apresentado os agradecimentos aos apoiadores desse artigo.

2. Referencial Teórico

O ambiente da Indústria 4.0 é definido não só pela automação industrial decorrente de dispositivos IIoT, mas também pela integração de inteligência artificial[Sellitto 2002], robótica e computação em nuvem. Neste contexto se insere o FASTEN, que é um fra-

mework para a Indústria 4.0 responsável pela integração de dispositivos IIoT com ferramentas de análise prescritiva e de otimização, para o auxílio na tomada de decisão e desenvolvimento de produtos para clientes únicos [Costa et al. 2020].

A arquitetura do FASTEN é composta por três níveis. O nível de borda, onde se encontram os dispositivos IIoT, o nível da plataforma, que é composta pelos middleware de conexão dos robôs à nuvem, de ordenação de cada solicitação e resposta da plataforma e os bancos de dados que armazenam as informações dos dispositivos IIoT e a terceira camada é responsável pelo nível empresarial, composta por diversos aplicativos, com a funcionalidade de gerenciar e analisar o dados e as informações.

O projeto FASTEN trouxe avanços no uso de dispositivos IIoT mas as questões de segurança das informações trafegadas ainda eram um desafio a ser tratado, uma vez que o framework FASTEN não possui uma camada de validação de identidade das requisições realizadas para a produção. Essas requisições são realizadas por um operador , e são enviadas para a plataforma de otimização do framework, que ordena e distribui as ordens de serviço por suas respectivas regiões.

Para garantir que somente requisições válidas sejam realizadas, mantendo a autenticidade de identidade dentro do framework, uma possível abordagem é a utilização da tecnologia de *blockchain* [Nakamoto 2008]. Essa tecnologia utiliza um banco de dados distribuído, também conhecido como livro razão global, que consiste em uma lista de transações agrupadas juntas, criptograficamente em uma cadeia de blocos imutável (*blockchain*) [Hileman and Rauchs 2017].

O *blockchain* utiliza o conceito de *Proof-of-Work* (prova de trabalho) para realizar a validação das transações realizadas na rede. Este conceito é um protocolo criptográfico que requer que todos (ou uma certa quantidade de) os membros de uma rede validem qualquer transação que seja emitida dentro dessa rede, para provar que uma quantidade de esforço computacional foi despendido e um consenso foi alcançado.

Uma rede *blockchain* pode ainda ser caracterizada como pública ou privada. A rede pública não requer nenhum tipo de autenticação para um novo usuário fazer parte da rede. Isso permite que qualquer um possa ingressar e tentar emitir uma transação dentro da rede. Já em rede privada, somente os usuários que forem autorizados a ingressar podem fazer parte da rede e emitir transações. Este modelo de rede blockchain é mais adequado a empresas que desejam manter um alto nível de governança sobre sua rede.

Transações em uma rede *blockchain* são quaisquer alterações de valores agregados a membros desta mesma rede. Estes valores são particulares de cada rede, e podem ser um valor monetário, informações sobre produtos ou documentos. Existem vários frameworks para implementação da tecnologia *blockchain*. Dentre eles, o Hyperledger Fabric [Fabric 2021].

O Hyperledger Fabric é uma plataforma de tecnologia de código aberto modular e configurável, projetada para o ambiente empresarial, com o foco na construção de aplicações em cadeia de blocos privados e permissionados [Burle 2019]. A plataforma opera baseada na premissa de contratos inteligentes (*chaincode*), em uma rede *blockchain* privada. A escolha dessa plataforma se deve a sua natureza permissiva, à programação em linguagens de uso geral e ao processamento em tempo real.

Na rede do Hyperledger Fabric cada componente e atores possuem suas identidades e políticas que definem controle de acesso e governança. na rede *blockchain*, essas políticas permitem que os membros venham a aceitar ou rejeitar mudanças na rede, no canal ou no contrato inteligente. As aplicações do Hyperledger Fabric, utilizando o SDK (*software development kit*), oferecem suporte somente a efetuar um pedido de transação na rede e de consulta. As operações administrativas são executadas através das ferramentas CLI (*command line input*) [Fabric 2021].

3. Solução Proposta

Detalhamos a seguir a implementação da rede *blockchain* utilizando o Hyperledger Fabric, para auxiliar nos protocolos de segurança do projeto H2020 FASTEN. Através da utilização do protocolo PKI *(Public Key Infrastructure*) [Weise 2001] é oferecido suporte para que as transações possam ocorrer na rede. Somente uma autoridade de certificação (*certificate Authority*) é capaz de repassar as informações de validação para os membros da rede.

Os membros da rede utilizam os contratos inteligentes (*Smart Contract*) para manter a integridade dos dados, através de uma arquitetura (executa-ordena-valida). A arquitetura permite a execução de uma transação e verifica sua validade através do protocolo de consenso, com a finalidade de ser inserida no livro-razão.

Na Figura 1 apresentamos uma visão geral da arquitetura para a incorporação dos contratos inteligentes via Hyperledger Fabric no contexto do projeto FASTEN, de modo que o acesso aos dispositivos IIoT seja protegido pela camada de validação da rede *blockchain*. O Hyperledger Fabric age, impedindo que algum *malware* tenha acesso aos dados da rede, seja se passando por um operador ou um dispositivo IIoT. Dessa forma, podemos garantir que somente quem tem autorização possa trafegar dados no ambiente FASTEN. Para isso, utilizamos o processo de validação de transação, conhecido como *Proof-of-Work* (prova de trabalho), do Hyperledger Fabric, para que todas as transações de dados sejam validadas e não possuam nenhuma falha. Assim, só após a validação, as transações podem ser passadas para os dispositivos de IIoT presentes na rede.

Como resultado, é possível verificar que a integridade dos dados, por meio deste mecanismo de assinaturas digitais, certifica a disponibilidade e confidencialidade das informações presentes entre as comunicações dos dispositivos. Assim, todas as transações de uma rede *blockchain* são mantidas de forma distribuída pelos membros da rede.

3.1. Projeto

O enfoque do projeto detalhado neste artigo está na criação de uma solução que atue em paralelo com o FASTEN, para auxiliar no gerenciamento da rede. Através dele o usuário pode, além de criar e gerenciar a rede, além de definir o seu próprio contrato inteligente.

Foi desenvolvida uma série de algoritmos para automatizar a criação dos arquivos de configuração e a própria rede do Hyperledger Fabric, e para auxiliar na utilização desses algoritmos foi desenvolvida uma interface simples.

O intuito da solução proposta é que o FASTEN possua uma camada de segurança através do Hyperledger Fabric, onde informações das requisições de produção das peças tenham um grau de segurança sobre a autenticidade de identidade no momento em

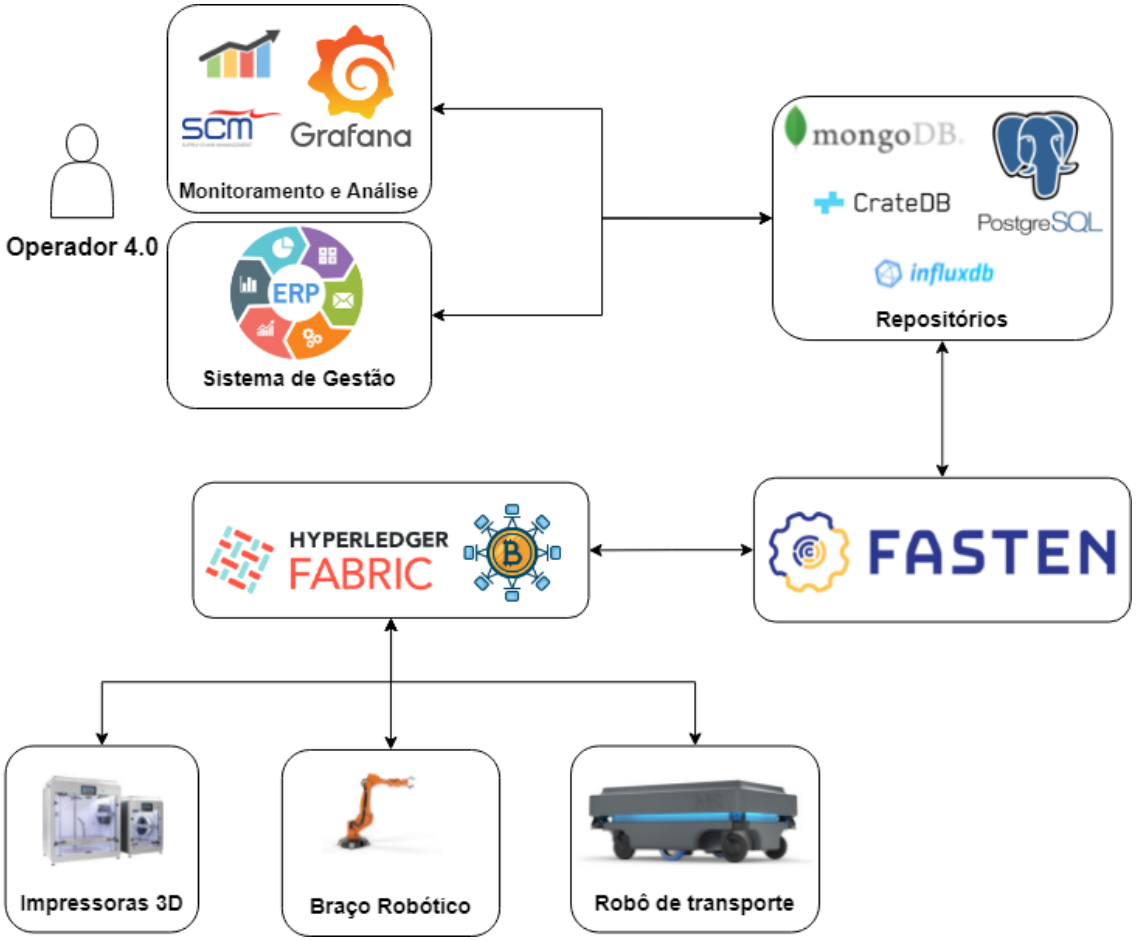

Figura 1. Arquitetura Proposta FASTEN - Contratos Inteligentes

que esses dados estão sendo encaminhadoa para os dispositivos IIoT, responsáveis pela fabricação das peças. Essa segurança é mantida pelo padrão de *blockchain* privado do Hyperledger Fabric, e pelo "*chaincode*", que segue padrões internos para cada tipo de Indústria.

Na Figura 2 apresenta uma representação simples do fluxo de dados no ambiente proposto pelo FASTEN com a incorporação do Hyperledger Fabric. Nele uma requisição é feita pelo usuário por meio de uma aplicação para utilizar um recurso, que no caso é um dispositivo IIoT. Esta requisição possui informações como identificação do requerente, localidade, data e hora, qual recurso será utilizado, e qual operação deve ser realizada (como uma impressão 3D). O framework FASTEN encaminha estes dados para a rede do Hyperledger Fabric que fará a autenticação da requisição. Se a requisição for válida, ela será encaminhada então para execução no dispositivo, que retornará a resposta da tarefa, caso consiga realizá-la ou não.

Como aplicação, o usuário pode iniciar ou finalizar a rede, criar e conectar a um canal para comunicação e instalar o chaincode a ser utilizado naquele meio. Em complemento a esse sistema, temos uma área onde um administrador da rede poderá cadastrar os usuários, dispositivos IIoT e enviar transações na rede com as determinadas atribuições. O cadastro de usuário é feito informando o nome, a descrição do usuário e uma chave

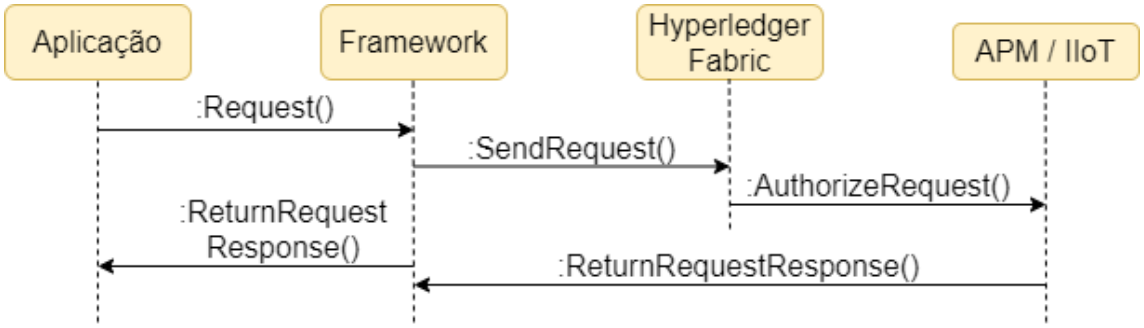

Figura 2. Fluxo de dados no ambiente FASTEN

pública gerada de forma automática e com um mecanismo de validação do usuário. O cadastro dos dispositivos IIoT é semelhante ao de usuários. Além das mesmas informações presentes para o usuário o dispositivo também recebe o tipo e operação que ele realiza.

Na Figura 3 é apresentada a interface que ilustra a execução de uma transação na rede. Conforme é apresentado na interface é informada a chave pública do usuário e do dispositivo IIoT e, por último, qual operação será executada.

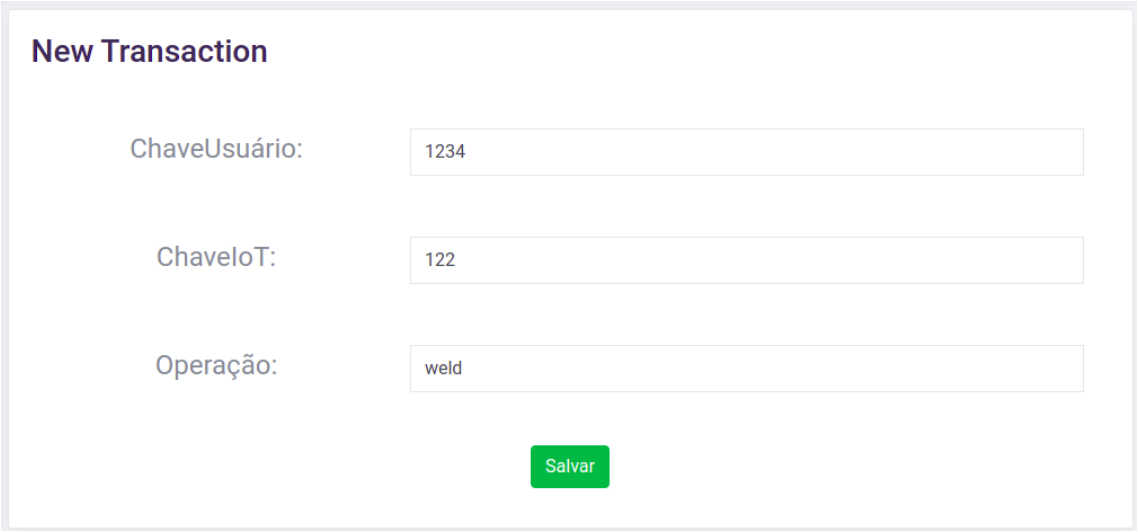

Figura 3. Interface de uma nova transação na rede usada na simulação

Na Figura 4 apresentamos uma tela de log de todas as transações que foram executadas na rede informando a chave do usuário (*userPKI*), a chave do dispositivo (*IoTPKI*), qual a operação realizada (*task*), o horário que foi realizada em *timestamp* e o status da transação. Através dessas informações é possível gerar dados estatísticos para que o gerenciamento da indústria consiga executar análises sobre os estados das transações.

Como prova de conceito inicial, foram realizadas algumas simulações do ambiente. Nos experimentos realizados em um ambiente simulado, foram testados os seguintes conjuntos de entradas:

1. Usuário válido, dispositivo cadastrado e operação válida;
2. Usuário invalido, dispositivo cadastrado e operação válida;
3. Usuário válido, dispositivo não cadastrado e operação válida;

Transactions

UserPki	IoTPki	Task	Timestamp	Status
c1eb3836-ef00-43a4-9f68-bbcc65ce7ecd	6eb28398-8698-46f0-8a94-78c67f8c04e7	print	1623981645473	invalid user
c1eb3816-ef00-43a4-9f68-bbcc65ce7ecd	6eb28398-8698-46f0-8a94-78c67f8c04e7	print	1623981660261	success
c1eb3816-ef00-43a4-9f68-bbcc65ce7ecd	6eb28398-8698-46f0-8a94-78c67f8c04e7	print	1623981661143	success
539a8b63-1747-441d-8e2f-927b6f12f193	6eb28398-8698-46f0-8a94-78c67f8c04e7	print	1623981697497	invalid user
ae3da5d0-a194-49cb-932b-9e7fdcf6c524	19b936dc-c8b1-402a-8eaf-55dd6c17b846	weld	1623981714942	success
c1eb3816-ef00-43a4-9f68-bbcc65ce7ecd	6eb28398-8228-46f0-8a94-78c67f8c04e7	print	1623981747939	iot/task not find
c1eb3816-ef00-43a4-9f68-bbcc65ce7ecd	6eb28398-8698-46f0-8a94-78c67f8c04e7	printt	1623981759343	iot/task not find
c1eb3816-ef00-43a4-9f68-bbcc65ce7ecd	6eb28398-8698-46f0-8a94-78c67f8c0447	print	1623981776673	iot/task not find
c1eb3816-ef00-43a4-9f68-bbcc65ce7ecd	68c99c30-567a-4225-b366-77418feaee98	print	1623981793043	success
c1eb3816-ef00-43a4-9f68-bbcc65ce7ett	6eb28398-8698-46f0-8a94-78c67f8c04e7	print	1623981846887	invalid user
c1eb3816-ef00-43a4-9f68-bbcc65ce7ecd	6eb28398-8698-46f0-8a94-78c67f8c04e2	print	1623981856247	iot/task not find

Figura 4. Log das Transações em uma rede

4. Usuário válido, dispositivo cadastrado e operação inválida;

Para o caso 1 o sistema retorna um sucesso (*success*) e realiza essa transação na rede *blockchain*. Para os casos 2, 3 e 4 o sistema não realiza a transação, e retorna um erro de usuário inválido (*invalid user*), dispositivo não encontrado (*iot/task not found*), e operação inválida, respectivamente (*iot/task not found*). Com base nos resultados obtidos conseguimos verificar a segurança fornecida pelo Hyperledger Fabric, atestando que somente um usuário e um dispositivo que atendam os requisitos da rede executem uma transação na rede.

4. Conclusão e Trabalhos Futuros

Nesse artigo, apresentamos uma solução visando a segurança de dados para processos relacionados à Indústria 4.0. Especificamente, foi apresentada uma solução para segurança no contexto do projeto H2020 FASTEN, considerando dispositivos IIoT. Com base nos resultados obtidos, há evidências de que o Hyperledger Fabric fornece uma camada extra de validação para o meio de comunicação das indústrias.

Como trabalhos futuros, é desejável que estudos experimentais mais detalhados sejam realizados. Além disso, pretendemos estender a solução proposta, considerando a automatização dos processos, facilitando o uso da tecnologia do Hyperledger Fabric em contextos mais amplos.

5. Agradecimentos

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001, UFJF, CNPq, e FAPEMIG.

Referências

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen,

B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolic, M., and Yellick, J. (2018). Hyperledger fabric: A distributed operating system for permissioned blockchains. *EuroSys '18: Proceedings of the Thirteenth EuroSys Conference*, (30):1–15. Available at https://dl.acm.org/doi/10.1145/3190508.3190538.

Burle, L. M. (2019). Um estudo de caso em cadeias de blocos: principais mecanismos de consenso e a plataforma Hyperledger Fabric. Trabalho de Conclusão de Curso (Graduação em Engenharia de Telecomunicações), UFF (Universidade Federal Fluminense), Rio de Janeiro, Brasil.

Coelho, R., Braga, R., David, J. M., Campos, F., and Ströele, V. (2019). Blockflow: Trust in scientific provenance data. In *Anais do XIII Brazilian e-Science Workshop*, Porto Alegre, RS, Brasil. SBC. https://sol.sbc.org.br/index.php/bresci/article/view/10033.

Costa, F. S., Nassar, S. M., Gusmeroli, S., Schultz, R., Conceição, A. G. S., Xavier, M., Hessel, F., and Dantas, M. A. R. (2020). Fasten iiot: An open real-time platform for vertical, horizontal and end-to-end integration. *Sensors*, 20(19). https://www.mdpi.com/1424-8220/20/19/5499.

Fabric, H. (2021). Hyperledger. https://hyperledger-fabric.readthedocs.io/en/release-2.2/blockchain.html.

Gilchrist, A. (2016). *Industry 4.0: the industrial internet of things*. Springer.

Hang, L. and Kim, D.-H. (2019). Design and implementation of an integrated iot blockchain platform for sensing data integrity. *Sensors*, 19(10). https://www.mdpi.com/1424-8220/19/10/2228.

Hileman, G. and Rauchs, M. (2017). Global blockchain benchmarking study. *SSRN*. Available at SSRN: https://ssrn.com/abstract=3040224 or http://dx.doi.org/10.2139/ssrn.3040224.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://www.klausnordby.com/bitcoin/Bitcoin_Whitepaper_Document_HD.pdf.

Rodrigues Pereira, A., Dalmarco, G., and G. Soares Alcalá, S. (2018). Fasten -flexible and autonomous manufacturing systems for custom- designed products. Available at https://www.atmosphere-eubrazil.eu/.

Sellitto, M. A. (2002). Inteligência artificial: uma aplicação em uma indústria de processo contínuo. gest. prod. 9(3). https://doi.org/10.1590/S0104-530X2002000300010.

Weise, J. (2001). Public key infrastructure. In *SunPSSM Global Security Practice Sun BluePrints™ OnLine*. http://highsecu.free.fr/db/outils_de_securite/cryptographie/pki/publickey.pdf.