République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université de Bejaia
Faculté des Sciences Exactes
Département d'Informatique

PROJET DE FIN DE CYCLE

en vue de l'obtention du diplôme de
Master recherche en informatique spécialté Réseaux et Sécurité.

Thème:

Proposition d'une technique de protection des chaînes de production

présenté et soutenue le 30/06/2025 par :

M. SACI Missipssa

encadré par :

Dr. HAMZA Lamia *M.C.A - U.A/Mira Béjaia*

jury :

Présidente	Dr. Zammouche Djamila	M.C.B - U.A/Mira Béjaia
Examinatrice	Dr. Yaici Malika	M.C.B - U.A/Mira Béjaia
Examinatrice	Dr. Aloui Soraya	M.C.A - U.A/Mira Béjaia
Examinatrice	Dr. Mammeri Souhila	M.C.B - U.A/Mira Béjaia

Année universitaire 2024-2025

Table des Matières

Table des figures

Liste des abréviations

- **ICS** : Industrial Control System - Système de Contrôle Industriel
- **SCADA** : Supervisory Control And Data Acquisition — Système de Contrôle et d'Acquisition de Données
- **DCS** : Distributed Control System - Système de Contrôle Distribué
- **PLC** : Programmable Logic Controller - Automate Programmable
- **OT** : Operational Technology - Technologie Opérationnelle
- **IT** : Information Technology - Technologie de l'Information
- **IoT** : Internet of Things - Internet des Objets
- **IA** : Intelligence Artificielle
- **RTU** : Remote Terminal Unit - Unité Terminale à Distance
- **Data Historian** : Système de stockage d'historique industriel
- **HMI** : Human–Machine Interface - Interface Homme-Machine
- **CCTV** : Closed-Circuit Television - Vidéosurveillance en circuit fermé
- **RSSI** : Responsable de la Sécurité des Systèmes d'Information
- **RS-232** : Recommended Standard 232 - Norme de communication série
- **RS-485** : Recommended Standard 485 - Variante de la norme série multipoint
- **Modbus** : Protocole de communication série maître-esclave
- **TCP/IP** : Transmission Control Protocol / Internet Protocol - Protocole Internet
- **PDU** : Protocol Data Unit - Unité de Donnée de Protocole
- **Modbus RTU** : Modbus Remote Terminal Unit - Modbus via communication série
- **Modbus ASCII** : Modbus American Standard Code for Information Interchange - Modbus codé ASCII
- **Modbus TCP** : Modbus Transmission Control Protocol - Modbus sur réseau IP
- **DNP3** : Distributed Network Protocol version 3 - Protocole de Réseau Distribué version 3
- **CRC** : Cyclic Redundancy Check - Contrôle de Redondance Cyclique
- **ETH** : Ether - Cryptomonnaie native de la blockchain Ethereum
- **Smart Contract** : Contrat intelligent - Programme autonome sur la blockchain
- **Chaincode** : Contrat intelligent privé dans Hyperledger Fabric

- **API** : Application Programming Interface - Interface de Programmation d'Applications
- **CDBF** : Centre de droit bancaire et financier
- **IBM** : International Business Machines
- **CA** : Certificate Authority - Autorité de Certification
- **MSP** : Membership Service Provider — Fournisseur de Services d'Adhésion
- **WSL2** : Windows Subsystem for Linux version 2 - Sous-système Windows pour Linux version 2

Introduction générale

L'Industrie 4.0, souvent appelée la quatrième révolution industrielle, est caractérisée par une transformation numérique de l'industrie où l'automatisation, la connectivité et l'analyse intelligente des données transforment les méthodes de production. Les systèmes de contrôle industriel (ICS, Industrial Control Systems, en anglais), qui garantissent la supervision, la gestion et l'automatisation des processus industriels, sont au centre de cette révolution. Que l'on parle de systèmes de contrôle et d'acquisition de données (SCADA, Supervisory Control And Data Acquisition, en anglais), de systèmes de contrôle distribués (DCS, Distributed Control Systems, en anglais) ou de contrôleurs logiques programmables (PLC, Programmable Logic Controllers, en anglais), ces technologies se sont imposées comme des éléments essentiels pour la performance et la compétitivité dans le domaine industriel. Toutefois, cette libéralisation technologique, amplifiée par l'interconnexion croissante entre les technologies opérationnelles (OT, Operational Technology, en anglais) et les technologies de l'information (IT, Information Technology, en anglais), entraîne de nouveaux périls en matière de cybersécurité. Initialement destinés à fonctionner dans des environnements confinés, les ICS sont maintenant connectés à des réseaux plus étendus, voire à Internet. Ils se retrouvent alors confrontés à des menaces pour lesquelles ils n'étaient pas initialement équipés. Ces dernières années, les assaults dirigés contre des infrastructures essentielles se sont intensifiés, engendrant parfois des répercussions dévastatrices sur la production, la sûreté des opérateurs et l'environnement. Aujourd'hui, la sécurisation des systèmes industriels est devenue une préoccupation stratégique cruciale, tant pour les sociétés que pour les gouvernements. Dans ce cadre, les technologies de la blockchain ouvrent des perspectives innovantes et encourageantes pour faire face aux défis contemporains. Grâce à leur caractère décentralisé, transparent et inaltérable, elles offrent la possibilité de concevoir des systèmes de contrôle plus robustes, traçables et dignes de confiance. Hyperledger Fabric, un framework modulaire développé par la Linux Foundation, est l'une des plateformes blockchain les plus appropriées aux contextes industriels. Hyperledger Fabric, qui a été élaboré surtout pour les consortiums d'affaires, présente des caractéristiques sophistiquées comme les canaux privés, les contrats intelligents (smart contracts, en anglais) et un contrôle d'accès granulaire. Ces spécificités le rendent judicieux à adopter dans une perspective de sécurisation des chaînes de production. Ce mémoire aborde ce sujet et aspire à suggérer une stratégie de sécurisation des milieux industriels fondée sur Hyperledger Fabric, en se basant sur l'exemple inspiré de l'organisation observée au sein de la SARL IBRAHIM et Fils - IFRI, une entreprise locale spécialisée dans la production d'eau minérale. Bien que cette entreprise ne constitue pas un cas d'étude formel dans ce travail, les observations effectuées sur son infrastructure de production ont permis de concevoir une proposition réaliste et adaptée, en réponse aux défis identifiés sur le terrain. La démarche développée dans ce mémoire vise ainsi à apporter une solution concrète, à forte valeur ajoutée, notamment en matière de traçabilité, de sécurité des données et de gestion des anomalies au sein des chaînes de production. Pour aborder cette question, le mémoire est organisé en trois chapitres complémentaires :

Le premier chapitre présente les systèmes de contrôle industriels. Il traite des principes de base et des structures courantes des ICS, met en lumière leur importance cruciale dans les procédures industrielles, et se concentre sur les défis de sécurité auxquels ils font face actuellement. On accorde une grande importance à l'évolution des menaces, aux vulnérabilités propres à ces systèmes, et aux exigences de sécurité dans des situations critiques.

Le chapitre deux se focalise sur la revue de littérature concernant Hyperledger Fabric. Ce document expose les principes fondamentaux de cette technologie blockchain, ses modes d'opération, ses caractéristiques distinctives en comparaison avec d'autres solutions blockchain, ainsi que les motifs qui justifient son adoption dans des applications industrielles. Il traite également des applications récentes de ce framework dans des environnements privés.

Le chapitre trois constitue la partie applicative du mémoire. Il offre une architecture de sécurité décentralisée destinée à un contexte industriel, basée sur Hyperledger Fabric. Cette approche comprend l'établissement de canaux séparés pour la gestion standard de la production et le suivi des anomalies, ainsi qu'un contrat intelligent qui garantit l'enregistrement et le contrôle des palettes tout au long du processus industriel. La conception de cette solution, inspirée des réalités observées à la SARL IBRAHIM et Fils - IFRI, vise à démontrer comment la blockchain peut accroître la transparence, la crédibilité et la sûreté au sein d'une chaîne de production tout en tenant compte des contraintes réelles du terrain.

Cette recherche vise à prouver que l'adoption de la blockchain dans le secteur industriel ne constitue pas uniquement une solution technologique à un enjeu de sécurité. Elle représente également un moteur d'innovation organisationnelle, capable de réinventer les processus industriels en mettant l'accent sur les valeurs de confiance, d'auditabilité et de souveraineté des données.

Chapter I

Introduction aux systèmes industriels

1 Introduction

De plus en plus, les systèmes industriels adoptent des technologies de l'information, notamment l'IoT (Internet of Things, de l'anglais : Internet des Objets), L'IA (Intelligence Artificielle), le big data et autres. Malgré leur évolution en termes de connectivité et de rapidité d'exécution grâce à l'émergence de l'informatique dans le secteur industriel, il est primordial de prendre en compte que, depuis que ces systèmes sont liés à l'informatique, on rencontre de plus en plus les mêmes problèmes de sécurité qu'on rencontre dans les systèmes d'informations traditionnels [4],mais le soucis repose sur le faite que les systèmes industriels n'ont pas été conçus pour faire face aux danger et menaces liés à ces technologies[3]. Contrairement à un système d'information, attaquer un système industriel ou un ICS (Industrial Control System, de l'anglais : Système de Contrôle Industriel) ne cible non seulement les informations contenues dans ces systèmes, mais cible plutôt leur sécurité physique, la santé et la sécurité des consommateurs voire même des travailleurs, et peut aller jusqu'à causer des dégâts environnementaux et économiques[1].

2 Axes de l'industrie

Pour parler des technologies mises en œuvre dans les systèmes industriels, il est important d'avoir une idée de départ sur ce qu'est l'industrie et quelles sont ses particularités. Lorsqu'on parle d'industrie, on a tendance à imaginer une usine ou une fabrique avec une chaine de production. Mais le terme est beaucoup plus large, c'est pour cela que des spécialistes ont défini deux axes principaux pour définir les secteurs de l'industrie, qui consistent en les industries de fabrication (manufacturing industries : en anglais) et les industries de distribution (distribution industries : en anglais)[4].

2.1 Industries de fabrication

Les industries de fabrication consistent en de très larges secteurs diversifiés avec différents processus qui sont présentés sous deux catégories : les processus de fabrication continue et les processus de fabrication par lot[4] [5].

2.1.1 Processus de fabrication continue

Il s'agit d'un processus de production sans interruption, c'est-à-dire que le produit est fabriqué du début jusqu'à la fin sans interruption. Ce type de processus s'exécute en mode continu

où, généralement, l'objectif est d'obtenir à la fin un produit sous différents niveaux. Des exemples typiques de ce genre de fabrication incluent : le raffinage du pétrole, la fusion de métaux, la distillation dans une usine chimique, etc. Ce type de processus se distingue par une grande fluidité, assurant une vitesse de fabrication optimale, bien qu'il implique un coût d'installation très élevé.

2.1.2 Processus de fabrication par lot

Le processus de fabrication par lot est un processus avec interruption, c'est-à-dire qu'un produit a un début et une fin sur chaque niveau, et chaque niveau est dépendant de son prédécesseur. Un processus par lot comporte des étapes de début et de fin clairement définies, avec la possibilité d'atteindre un état stable temporaire pendant certaines étapes intermédiaires. On fait appel à ce genre de processus, généralement, pour garantir un certain niveau de conformité aux normes réglementaires. Parmi les processus typiques de fabrication par lot, on retrouve notamment la production alimentaire et la production de médicaments. Contrairement au processus continu, ce type de processus se caractérise par un coût d'installation réduit, mais une vitesse de fabrication plus lente.

2.2 Industrie de distribution

Par définition, la distribution est une activité permettant de transiter un produit dans son état final vers un point de consommation ou d'acquisition depuis son point de production [7]. En industrie, la distribution est un concept clé pour connecter les industries de fabrication à leurs fournisseurs, leurs clients ainsi qu'à leurs sous-traitants. En d'autres termes, il s'agit du maillon fort de la chaine d'approvisionnement (supply chain en anglais) [6]. Des exemples typiques se traduisent par des applications concrètes, telle que la chaîne logistique, le transport (marchandise, livraison, etc.). Ce type d'industrie s'étend jusqu'à nous atteindre dans nos vies quotidiennes, et ce, par le biais de la distribution d'eau, de gaz, d'électricité, etc.

3 Informatique appliquée à l'industrie

Afin de comprendre comment l'industrie bénéficie des merveilles qu'apporte l'informatique dans son secteur, il est nécessaire de comprendre ce que la technologie de l'information, ainsi que sont homologue, à savoir la technologie opérationnelle.

3.1 Technologies de l'information

La technologie de l'information (Information Technology, en anglais) est un terme général qui désigne l'ensemble des ressources, voir même d'infrastructures, de processus, de systèmes mis en œuvre pour la création, la gestion, le stockage, la sécurisation et l'échange de données. En d'autres termes, il s'agit de tous systèmes servant à traiter l'information numérique.

3.2 Technologies opérationnelle

Contrairement à la technologie de l'information qui sert à la gestion de l'information, la technologie opérationnelle (Operationnal Techonology (OT), en anglais) souvent désigné par "Systèmes d'information industriels" se traduit en un ensemble de processus, de systèmes et de dispositif physiques qui sont mis en œuvre afin de piloter ainsi que de superviser des

évènements et des installations physiques dans un milieu industriel [3] [9]. La figure I.1 illustre les différences clés entre un environnemnt IT et un environnement OT.

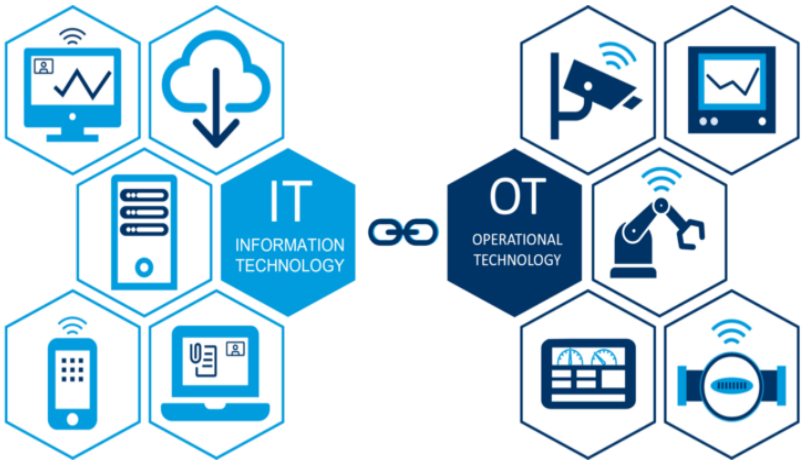

Figure I.1: Technologies de l'information et Technologies opérationnelle

3.3 Technologies de l'information vs technologies opérationnelle

Les systèmes d'informations ainsi que les systèmes opérationnelles présentent des distinctions considérables. Ci-dessous, nous avons énuméré les différences clés entre ses deux types de technologies[3] :

- **Objectif des systèmes :** tel cité dans leurs définitions respectives ci-dessus, la technologie de l'information se caractérise par le traitement de la donnée numérique, contrairement à la technologie opérationnelle qui, elle, en plus du traitement de l'information, sert à manipuler également des installations physiques.

- **Contraintes :** les contraintes principales des IT sont généralement des contraintes métier, telles que les régulations, les exigences de conformité, etc., ainsi que des contraintes de confidentialité. En revanche, les OT sont contraints par le traitement en temps réel des opérations, la sûreté de fonctionnement ainsi qu'une disponibilité souvent exigée à 24 H/24 et 7 J/7.

- **Environnement et localisation géographique :** Bien que les systèmes IT soient souvent confinés dans des bureaux ou des salles serveurs sécurisés et climatisés, les OT quant à eux sont souvent placés dans des ateliers de production, exposés à la poussière, aux températures irrégulières, aux vibrations, aux produits nocifs, voire même aux travailleurs curieux qui ont tendance à bidouiller sur les composants.

- **Composition et hétérogénéité des composants :** les IT présentent des systèmes dits "durcis" contre les attaques informatiques, mais font face à une exigence capitale, qui est la compatibilité des composants. Par ailleurs, les OT sont des systèmes robustes, conçus souvent pour résister aux conditions difficiles des milieux industriels. Ils sont généralement caractérisés par la longévité de vie de leurs composants qui peut aller jusqu'à 10 ans, voire plus, mais présentent des lacunes contre les attaques informatiques.

3.4 Systèmes de contrôle industriels

Les systèmes de contrôle industriel (ICS : Industrial Control Systems) sont un terme général qui inclut plusieurs composants, qui sont combinés afin d'atteindre un objectif industriel [4]. Ces systèmes jouent un rôle essentiel pour assurer la connectivité des infrastructures industrielles ainsi que de leurs systèmes interdépendants, tout en assurant la supervision, le contrôle ainsi que la régulation des opérations [9].

Dans les secteurs industriels, on identifie plusieurs composants, tels que les systèmes de contrôle supervisé et d'acquisition de données (SCADA : Supervisory Control And Data Acquisition, en anglais), les systèmes de contrôle distribués (DCS : Distributed Control Systems, en anglais), ainsi que les automates programmables (PLC : Programmable Logic Controllers, en anglais). La figure I.2 présente les différentes composantes d'un environnement OT.

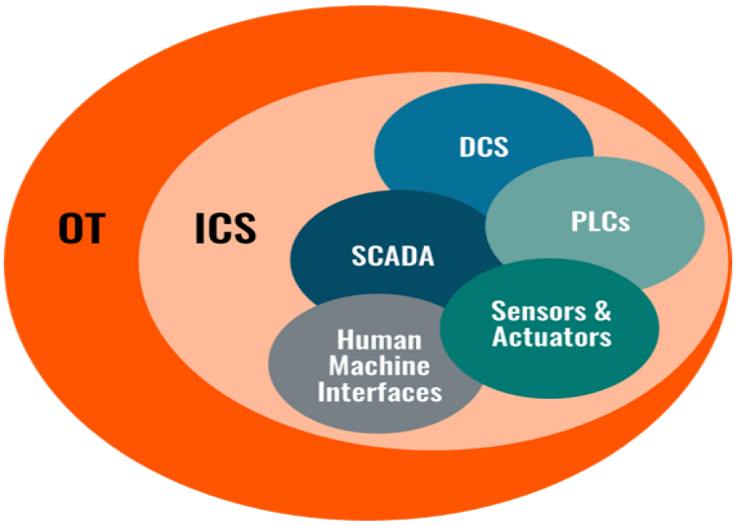

Figure I.2: Les systèmes de contrôle industriels ICS

3.5 Systèmes de contrôle supervisé et d'acquisition de données

Un système de contrôle supervisé et d'acquisition de données SCADA est un système informatique utilisé dans les milieux industriels, par exemple dans la production de gaz, l'approvisionnement d'eau, la production d'énergie électrique ainsi que la supervision des chaînes de production dans les usines, etc., afin de piloter et de superviser les actions effectuées par les équipements physiques. Par ailleurs, un système SCADA permet d'assurer la coordination des infrastructures [11], de collecter des données en temps réel, de surveiller les processus ainsi que de contrôler à distance les équipements [9]. Cela permet aux superviseurs de disposer d'une vision globale ainsi que de contrôler efficacement leurs infrastructures depuis une interface centralisée.

3.6 Système de contrôle distribué

Contrairement aux systèmes SCADA, qui peuvent couvrir de vastes zones géographiques, un système de contrôle distribué DCS est mis en œuvre afin de contrôler des systèmes de production situés en un même lieu géographique. [4][9].

Les DCS sont souvent utilisées dans des architectures de contrôle réparti, qui sont principalement présentes dans les industries dans le but de gérer des processus complexes ou continus. Ils combinent un niveau de supervision global avec des sous-systèmes spécialisés, où chacun est chargé de contrôler un aspect bien précis des opérateurs locaux.

3.7 Unité de Terminale à Distance

Dans un système de contrôle industriel, l'unité terminale à distance (RTU : Remote Terminal Unit, en anglais) joue un rôle crucial dans la manipulation des données, puisque c'est elle qui se charge de la collecte, de la conversion du signal analogique en signal numérique. Et ce, pour transmettre la donnée à un centre de contrôle où elles peuvent être soit stockées dans un *Data Historian*[1] ou affichés aux opérateurs. Elles peuvent également recevoir des signaux de contrôle depuis le centre de contrôle pour les transmettre aux capteurs du terrain[11]. Les RTUs les plus récentes ne se contentent plus de collecter et de transmettre des informations, mais elles offrent également des fonctionnalités supplémentaires. Par exemple, fixer un marquage temporel dans le but de réduire les risques liés à la latence.

3.8 Automates programmables

Les automates programmables (PLC : Programmable Logic Controller, en anglais) sont utilisés à la fois dans les systèmes SCADA et DCS comme composants de contrôle[4]. Ils peuvent contenir une logique et une programmation pour contrôler, en temps réel, des fonctions qui ne nécessitent pas forcément de communiquer avec les serveurs SCADA ou DCS. Conçus pour être placés soit côte-à-côte ou à la place des RTU[11], les PLC sont classés en fonction du nombre et du type des ports d'entrée/sortie qu'ils offrent.

3.9 Interface homme-machine

L'interface homme-machine (HMI : Human–Machine Interface, en anglais) permet aux opérateurs d'interagir avec les infrastructures des systèmes ICS. Connectée aux bases SCADA, elle fournit des visualisations et des métriques sur les performances, la maintenance et les schémas techniques. Les outils de visualisation de l'HMI incluent des diagrammes topologiques, des graphiques, des jauges, des cadrans, ou tout autre symbole technique pour représenter les éléments des processus. Elle peut même intégrer des images de caméras de vidéosurveillance CCTV (Closed-Circuit Television, en anglais), offrant ainsi aux opérateurs une vue directe des équipements surveillés et manipulés.

4 Analyse de la sécurité des systèmes industriels

Les systèmes de contrôle industriels modernes présentent de plus en plus de taux de connectivité à Internet qu'auparavant. Cependant, la convergence IT-OT ne cesse de se retourner au désavantage des entreprises industrielles, car elle étend les périmètres opérationnels des cyberattaquants, attirant ainsi un nombre croissant d'acteurs malveillants. Malgré son rapprochement de plus en plus étroit avec les technologies de l'information, ce type de

[1]**Data Historian:** est un système utilisé pour collecter et stocker les données issues de l'ICS, créant un historique complet des actions et événements. Il nécessite des serveurs puissants pour traiter des volumes de données souvent proches du big data.

technologie n'est pas encore complètement prêt à affronter les dangers et les risques liés à la cybercriminalité.

Dans ce qui suit, nous allons examiner en profondeur tout ce qui est lié à la cybersécurité des systèmes industriels.

4.1 La cybersécurité des ICS en chiffres

De nombreux géants de la cybersécurité ont mené des enquêtes sur le nombre d'attaques lancées sur des systèmes industriels ainsi que leur impact sur les entreprises. D'après le rapport rendu par les chercheurs des laboratoires Kaspersky pour le deuxième trimestre de 2024, dans lequel ils étudient les menaces et les attaques auxquelles les systèmes de contrôle industriels (ICS) ont été confrontés, plus de 23,5% des systèmes ICS dans le monde entier contiennent des objets malveillants[12]. Les régions les plus affectées au niveau mondial sont l'Afrique et le Sud-Est asiatique, avec plus de 30% d'environnements OT infectés. Rajoutons à cela que, d'après le rapport des mêmes laboratoires pour le deuxième semestre de 2022, les quatre pays les plus touchés par des incidents de sécurité liés aux ICS sont l'Éthiopie, l'Afghanistan, l'Algérie et le Turkménistan. La figure I.3 représente la liste des pays où des objets malveillants ont été signalés sur des ordinateurs OT, avec leurs pourcentages correspondants.

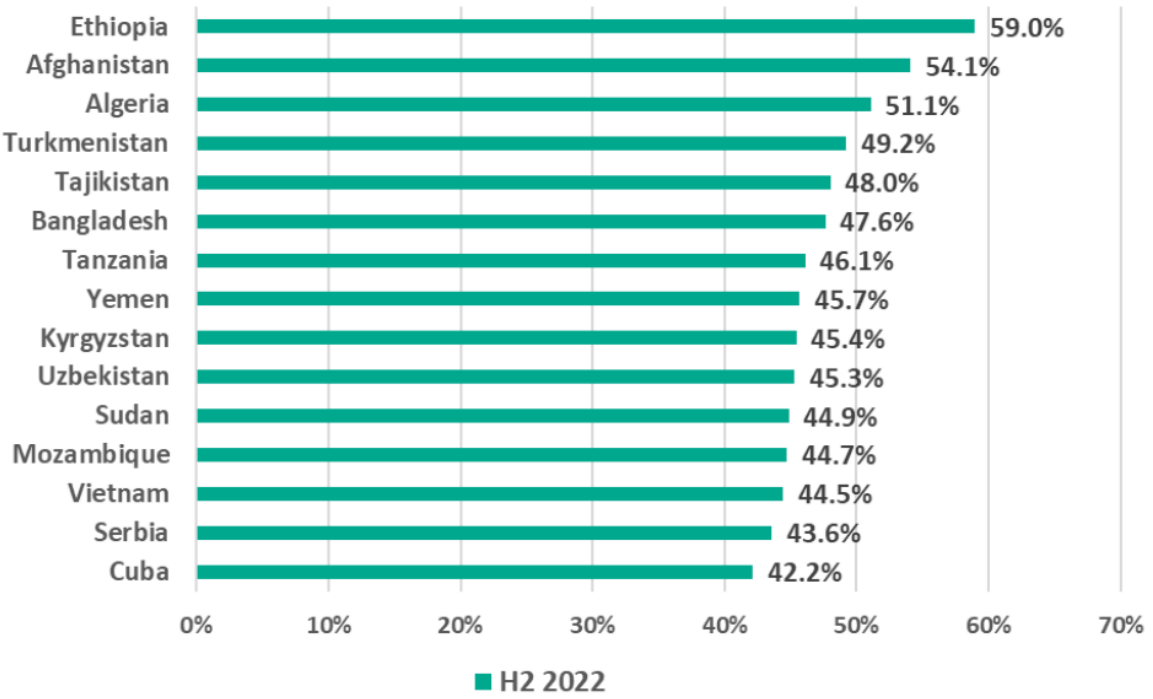

Figure I.3: 15 pays avec le plus haut pourcentage d'ordinateurs ICS bloquant des objets malveillants (S2 2022) [12]

De plus, selon le rapport rendu par Fortinet [13], après avoir mené une enquête internationale avec 550 professionnels en technologie OT, le nombre de personnes, voire d'entreprises, ayant signalé avoir subi au moins 6 intrusions par an a augmenté de 20% par rapport à l'année 2023, atteignant plus de 31% en 2024. Les mêmes spécialistes signalent aussi que les attaques deviennent de plus en plus sophistiquées, se basant sur des attaques de phishing ainsi que sur

d'usurpation d'identités à travers les emails. Et l'impact de ses intrusions sur les entreprises ne cesse d'accroître. La figure I.4 montre des statistiques de 2022, 2023 et 2024 résumant l'impact des attaques liées aux technologies opérationnelles sur la productivité, l'image de marque, le chiffre d'affaires, etc.

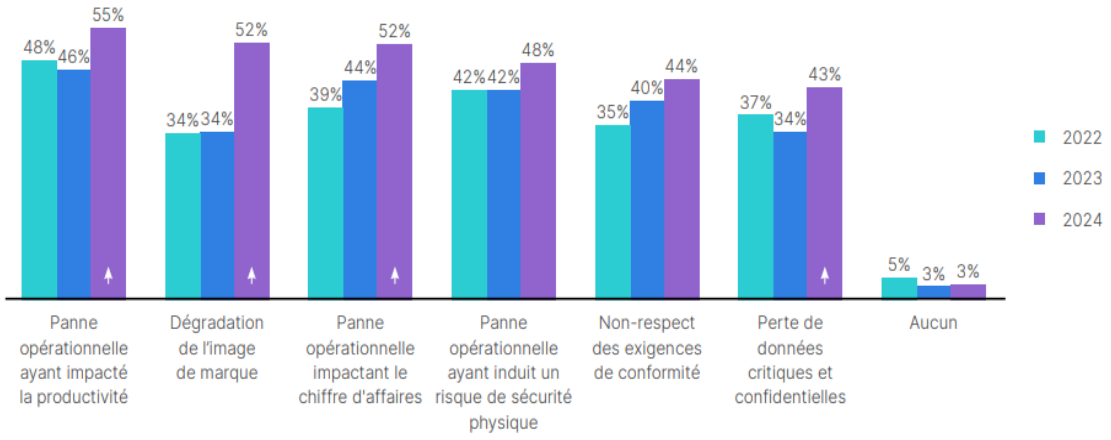

Figure I.4: Impact des intrusions sur les systèmes industriels [13]

4.2 Défis liés à la sécurité des technologies opérationnelle

Les principaux défis liés à la sécurité des technologies opérationnelle sont :

- **Manque de visibilité :** Tel cité précédemment, les réseaux de technologie opérationnelle se composent généralement d'équipements qui répondent à des cycles de vie largement plus importants que ceux des équipements des technologies de l'information (15 à 30 ans, voire plus, contre 3 à 4 ans pour les équipements IT). De plus, les entreprises possèdent très rarement des bilans sur leurs ressources OT à protéger [14]. Ceci entraîne des déficits quant à leur défense contre des attaques informatiques, et il est donc difficile d'évaluer les risques et vulnérabilités liées à ces technologies. Ce qui donne un manque de visibilité sur la sécurité des systèmes de contrôle industriels.

- **Manque de confiance et de collaboration entre les équipes IT et OT :** Dans de nombreuses entreprises, la cybersécurité dépend d'une collaboration stratégique entre le responsable de la sécurité des systèmes d'information (RSSI) et les équipes IT. Toutefois, ces acteurs possèdent rarement une expertise approfondie dans les technologies spécifiques au contrôle des processus opérationnels. Parallèlement, les équipes OT, souvent soucieuses de préserver l'intégrité de leurs réseaux, peuvent être tentées de restreindre l'accès, alimentant ainsi une méfiance mutuelle. Ce manque de confiance et l'absence de collaboration entre les départements OT et IT ne se contentent pas de limiter l'efficacité opérationnelle : ils exposent l'ensemble de l'organisation à des vulnérabilités majeures en matière de sécurité.

- **Absence d'expertise en sécurité informatique des équipes OT :** Dans les environnements OT, la priorité est souvent donnée à la disponibilité des systèmes, tandis que la confidentialité et l'intégrité des données passent au second plan. [14]. Cela s'explique par la nécessité de garantir la continuité de services essentiels. Pourtant,

cette approche diffère des pratiques IT, où ces trois aspects sont traités sur un pied d'égalité. Ce problème est aggravé par un manque de compétences en cybersécurité dans les équipes OT, qui ont du mal à repérer des menaces complexes. Si les attaques par malwares sont fréquentes, certaines plus discrètes modifient simplement les paramètres des processus industriels pour en perturber le fonctionnement. Ce manque de compétences en sécurité informatique expose donc les infrastructures critiques à des risques importants et croissants.

4.3 Exemples d'attaques concrètes sur les systèmes ICS

Il est impossible d'aborder la cybersécurité des systèmes de contrôle industriel (ICS) sans évoquer des exemples concrets d'attaques qui ont ciblé ces infrastructures critiques. En raison de leur rôle central dans des secteurs essentiels comme l'énergie, le transport ou l'eau, les ICS sont régulièrement la cible de cybermenaces sophistiquées, dont certaines ont marqué l'histoire par leur ampleur et leurs conséquences. Parmi ces attaques, on peut citer :

4.3.1 Stuxnet (2010)

Stuxnet est l'une des cyberattaques les plus médiatisées. Il s'agit d'un ver informatique, conçu pour cibler spécifiquement les systèmes ICS utilisant le protocole Siemens Step7 sur des automates programmables (PLC), et qui a saboté des centrifugeuses utilisées dans les installations nucléaires iraniennes. L'attaque a non seulement perturbé la production d'uranium, mais elle a aussi mis en lumière la vulnérabilité des infrastructures industrielles face aux cybermenaces[16].

4.3.2 BlackEnergy (2015)

Cette attaque a visé les infrastructures énergétiques en Ukraine. Les cybercriminels ont utilisé le malware BlackEnergy pour compromettre des systèmes SCADA, entraînant une panne d'électricité massive qui a affecté des centaines de milliers de foyers.

4.3.3 Triton/Trisis (2017)

Triton, également connu sous le nom de Trisis, est une attaque sophistiquée contre les systèmes de sécurité fonctionnelle. Elle a ciblé les contrôleurs de sécurité Schneider Electric Triconex, conçus pour prévenir des situations dangereuses dans des installations critiques, comme les usines chimiques ou pétrolières. L'objectif était de provoquer des pannes ou même des explosions en compromettant les mécanismes de sécurité.

4.3.4 Colonial Pipeline (2021)

Bien que l'attaque sur Colonial Pipeline soit principalement une attaque par ransomware, elle illustre l'impact indirect des cybermenaces sur les systèmes ICS. L'infection a conduit à la fermeture préventive d'un des principaux pipelines de distribution de carburant aux États-Unis, causant des perturbations majeures dans l'approvisionnement énergétique.

Ces exemples démontrent à quel point les ICS sont exposés à des attaques de plus en plus sophistiquées. La sécurisation de ces systèmes est donc une priorité absolue pour limiter les impacts potentiellement dévastateurs sur les infrastructures critiques et les économies nationales.

5 Protocoles des systèmes de contrôles industriels

Les protocoles des systèmes industriels sont des outils fondamentaux permettant la communication entre les différents équipements d'une chaîne de production. Ils définissent les règles et les standards pour assurer des échanges d'informations fiables, rapides et sécurisés entre capteurs, actionneurs et automates. Ces protocoles, indispensables à l'automatisation des processus, se déclinent en plusieurs types selon leur application et leurs spécificités techniques. Cette diversité rend nécessaire une classification précise ainsi qu'une analyse détaillée de leurs caractéristiques pour mieux comprendre leur rôle et leur adaptation aux besoins industriels.

5.1 Classification des protocoles

Dans cette section, nous allons présenter les classification des protocoles des systèmes de contrôles industriels :

5.1.1 Vendor-Specific

Cette catégorie définit des protocoles propriétaires qui sont spécifiques à leurs concepteurs. Ils ont été développés spécialement dans le but de fonctionner qu'avec des équipements construits par le même fabricant, ou bien des équipements de plusieurs fabricants. On retrouve beaucoup d'acteurs dans la conception de matériels industriels ainsi que leurs protocoles, parmi eux : Siemens avec Siemens S7 et Sixec H1 comme protocoles, Schneider Electric avec Foxboro, Tridium avec Niagara Tridium, ainsi que plein d'autres concepteurs qui utilisent des protocoles propres à eux[15].

5.1.2 Protocoles largement utilisés

Les protocoles largement utilisés (Widely Used Protocoles, en anglais) sont des protocoles qui sont non spécifiques à un concepteur d'équipements industriels et qui sont donc non propriétaires. Ce sont des protocoles qui peuvent être mis en place pour fonctionner avec n'importe quel équipement de contrôle industriel (conçu par n'importe quel fabricant). Parmi les protocoles que l'on peut retrouver dans cette catégorie, il y a : Modbus, DNP3, HART, etc.[18]

5.2 Caractéristiques des protocoles ICS

Tous les systèmes, interfaces et instruments d'un système ICS utilisent des protocoles différents pour la communication en temps réel et le transfert de données. Ces protocoles ont été conçus dans un premier temps pour une connexion série, mais, avec le temps, ils ont évolué pour prendre en charge et fonctionner sur les protocoles TCP/IP sur les réseaux Ethernet. Les protocoles suivants sont les plus utilisés : RS-232 et RS-485, Modbus, DNP3, ICCP.

5.2.1 RS-232 et RS-485

Parmi toutes les interfaces série du marché, RS-232 et RS-485 sont les plus anciennes et sont encore largement utilisées. RS-232 est principalement utilisé pour les besoins de faible vitesse sur de courtes distances. En raison de son faible coût, de sa conception simple et de l'espace suffisant pour plusieurs récepteurs, divers connecteurs sont disponibles pour se connecter à son interface. Avant le développement d'Ethernet, la sécurité n'était pas une préoccupation majeure pour les systèmes RS-232 et RS-485. Même aujourd'hui, ils sont rarement connectés

à Internet, ce qui constitue une protection contre les attaques. Les systèmes RS-485 exécutant Modbus TCP/IP sont connectés plus souvent, mais le risque est minime.

5.2.2 Modbus

Le Modicon Communication Layer (Modbus) est un protocole de la couche application développé en 1979 par Modicon (désormais Schneider Electric). Il utilise une architecture maître-esclave où le maître envoie des requêtes aux esclaves, qui répondent uniquement si une requête leur est adressée. Modbus repose sur trois types de PDU : Modbus Request (requête), Modbus Response (réponse en cas de succès) et Modbus Exception Response (réponse en cas d'erreur). Il peut être utilisé via plusieurs méthodes de communication :

- la communication série avec RS-232 et RS-485.
- la communication en réseau avec Ethernet utilisant TCP/IP.

Il existe trois variantes de Modbus : le **Modbus RTU** pour la communication série asynchrone, le **Modbus ASCII** pour la communication série, le **Modbus TCP** utilisé pour la communication sur réseaux IP. Le protocole Modbus TCP peut ajouter un en-tête pour la communication via Internet de deux manières : en conservant ou en retirant certaines informations d'adressage. Cependant, Modbus présente des limites : Il ne propose ni authentification ni chiffrement, et il peut saturer les réseaux avec trop de messages en raison de l'absence de mécanismes de suppression.

5.2.3 DNP3

DNP3, pour Distributed Network Protocol (protocole de réseau distribué, en français), a été développé en 1993 et est très répandu aux États-Unis et au Canada. Il fonctionne au niveau des couches application, liaison de données et transport. Il s'agit donc d'un protocole à trois couches. La conception de DNP3 s'est davantage concentrée sur la maximisation de la disponibilité du système que sur la confidentialité et l'intégrité. Au niveau de la couche de liaison de données, il est capable de détecter toute erreur dans la transmission de données au moyen d'un contrôle CRC. Des efforts ont également été faits pour fournir une authentification sûre au niveau de l'application. DNP3 possède une autre variante appelée DNP3 sécurisé, qui prend en charge l'authentification sécurisée et d'autres fonctionnalités de sécurité au niveau de l'application et est toujours recommandée à la place de DNP3.

5.2.4 ICCP

Le protocole ICCP (Inter-Control Communication Protocol, en anglais) est un protocole de la couche application développé en 1991 pour permettre l'échange de données en temps réel entre les stations électriques. Basé sur une architecture client-serveur, il facilite la connexion, la lecture, l'envoi d'informations, la configuration et le contrôle à distance. Il utilise une table bilatérale comme liste de contrôle d'accès pour valider les droits d'accès entre le client et le serveur. Fonctionnant sur des réseaux étendus, il est compatible avec différents protocoles de transport et fonctionne sur le port 102/TCP via Ethernet. Toutefois, il ne propose ni authentification ni chiffrement, ce qui le rend vulnérable aux attaques par déni de service.

6 Conclusion

Ce chapitre a permis de présenter les systèmes de contrôle industriel (ICS) dans leur globalité, en mettant en lumière leur rôle stratégique dans les infrastructures critiques. Nous avons également abordé les enjeux majeurs liés à la sécurité de ces systèmes, qui sont de plus en plus exposés à des cybermenaces sophistiquées. Les exemples concrets d'attaques, comme Stuxnet ou Triton, illustrent l'ampleur des risques et les conséquences potentielles sur la société et l'économie. Face à ces défis croissants, il est impératif d'adopter des stratégies de sécurisation robustes et adaptées aux spécificités des ICS. Cela inclut l'intégration des nouvelles tendances technologiques, telles que la blockchain, qui offre des solutions innovantes pour renforcer la résilience des systèmes face aux menaces actuelles et futures. Le renforcement de la sécurité des ICS ne constitue pas seulement une nécessité, mais une priorité absolue pour garantir la continuité et la fiabilité des infrastructures critiques.

Chapter II

Ètat de l'art

Traditionnellement liée aux cryptomonnaies, la technologie blockchain s'est vite étendue à d'autres domaines, notamment l'industrie où elle répond à des défis importants tels que la traçabilité, la transparence et la sécurité des données [17]. Dans un contexte de production où l'interconnexion des participants et des systèmes est prédominante, la blockchain offre la possibilité d'organiser des registres partagés, inaltérables et horodatés, augmentant ainsi la fiabilité des transactions sans avoir besoin d'une autorité centrale [18].

Hyperledger Fabric se démarque parmi les plateformes actuelles grâce à sa modularité, son architecture permissionnée et sa capacité à établir des politiques d'approbation personnalisées [19]. Ces attributs la rendent particulièrement appropriée pour des environnements industriels multisites, où plusieurs entités collaborent sur des processus essentiels tout en préservant leurs politiques internes de gouvernance [20]. Cependant, malgré ces bénéfices, l'emploi de Hyperledger Fabric dans le secteur manufacturier est encore faiblement documenté en raison du caractère confidentiel des projets, de la complexité technique des intégrations et des défis de performance relevés dans les publications [21][22].

En réponse à ces restrictions, une quantité proliférante de recherches scientifiques et techniques permet désormais d'examiner plus en détail les contributions et les contraintes de cette technologie. Ces recherches portent également sur l'incorporation de la blockchain dans les chaînes de production et sur l'amélioration des performances de Fabric. Elles offrent aussi des perspectives intéressantes lorsqu'on les associe à des initiatives qualité comme le Lean Six Sigma [23].

Cet état de l'art est structuré autour de quatre volets principaux : un premier qui s'intéresse à l'incorporation de la blockchain dans les processus de production, un second qui examine les performances de Hyperledger Fabric, un troisième qui traite des applications exemplaires dans l'industrie agroalimentaire, et enfin une dernière section qui explore la synergie entre la blockchain et les initiatives d'amélioration continue.

1 Histoire de la blockchain

L'origine de la blockchain demeure quelque peu incertaine. Des spécialistes estiment que la blockchain a commencé avec le lancement de la première cryptomonnaie, le Bitcoin, ainsi que la publication de son white paper par Satoshi Nakamoto[48]. D'autres estiment que son origine remonte à l'année 1991, avec la mise au point, par Stuart Haber et W. Scott Stornetta, d'une suite d'empreintes mathématiques publiée dans le New York Times, qui servait à prouver l'intégrité des données conservées. Cette expérience est vue comme la première blockchain en papier, toujours en cours depuis 1995[49].

Mais pour analyser, comprendre et suivre l'actualité de la blockchain, passons d'abord par un petit bout d'histoire sur l'évolution de la blockchain[50].

1.1 Blockchain 1.0

La première génération de blockchain est apparue avec le lancement des cryptomonnaies. Leur rôle principal était d'améliorer le système monétaire actuel en se basant sur la cryptographie asymétrique ainsi que sur les communications pair-à-pair au lieu de dépendre d'une entité centrale telle que les banques pour gérer et archiver les transactions. Elles se caractérisent par une décentralisation des réseaux, l'anonymat des utilisateurs, mais surtout par la transparence des transactions. En revanche, leur grand inconvenient est le fait qu'elles se basent sur le consensus proof-of-work (qui sera discuté juste après) pour valider les blocs, qui est gourmand en consommation de ressources.

1.2 Blockchain 2.0

Cette génération de blockchain est marquée par le lancement de la première plateforme de réseaux décentralisés, à savoir Ethereum, lancée par un jeune développeur russo-canadien appelé Vitalik Buterin. Cette plateforme ne se contente pas seulement d'offrir aux utilisateurs la possibilité d'échanger des fonts, mais elle va au-delà de cela. Elle permet à ses acteurs de créer des applications décentralisées avec lesquelles ils peuvent offrir leurs services en échange de fonds avec l'Ether (ETH) comme moyen de paiement sécurisé et décentralisé. Mais ça ne s'arrête pas ici : en plus de tout cela, cette plateforme introduit un nouveau concept qui est le smart contract.

1.3 Blockchain 3.0

Cette troisième génération n'est qu'une amélioration des générations précédentes, et ce en mettant en place quelques changements, tels que le remplacement du protocole de consensus proof-of-work par proof-of-stake, pour faciliter l'accessibilité et améliorer les performances du réseau blockchain ainsi que d'autres changements pour booster les performances et devenir applicable dans d'autres industries. Ces changements ont entraîné l'apparition de nouvelles architectures telles que le consortium ainsi que la cross-chain transaction. Mais surtout, ce qui a marqué cette génération, ce sont les régulations portant sur la conformité réglementaire, la gouvernance, la confidentialité et les smart contracts.

1.4 Blockchain 4.0

Les professionnels ne se sont pas encore mis d'accord sur la vision ou le futur de la blockchain. Certains pensent qu'elle va suivre le chemin des technologies disruptives telles que l'IA et l'IoT. D'autres estiment qu'elle doit suivre le chemin des générations précédentes en améliorant ses caractéristiques et ce, pour devenir plus efficace, scalable et accessible au grand public. En revanche, l'avènement des blockchains privées ainsi que l'introduction des DLT dans les milieux industriels peuvent chambouler les technologies IT et OT.

2 Réseau distribué ou réseau décentralisé

Les architectes, aujourd'hui, cherchent de plus en plus à construire des systèmes plus robustes et résistants, plutôt que de construire des structures avec seul un point de défaillance qui

fait tomber le système tout entier. C'est pour cela qu'au lieu de se tourner vers des systèmes centralisés où un seul nœud s'occupe des calculs et de la gestion des données, ils essaient de mettre en place des systèmes qui décentralisent ces calculs, et ce dans le but d'assurer la disponibilité et l'intégrité de leurs systèmes en se tournant vers les systèmes distribués et les systèmes décentralisés. Néanmoins, malgré la ressemblance de ses deux termes, des différences techniques et fonctionnelles se manifestent entre eux[48].

2.1 Système distribué

Dans un système distribué, si une partie du système est attaquée ou est défaillante, cela n'empêche le système de continuer de fonctionner. Dans ces mêmes systèmes, les calculs ne sont pas effectués par un seul nœud central, mais plutôt répartis sur un nombre d'unités ou de nœuds qui collaborent afin de réaliser des tâches et des calculs communs, et ce grâce à une communication instaurée entre ces entités.

2.2 Système décentralisé

Le premier principe des systèmes distribués qu'on vient d'aborder est le cœur même des systèmes décentralisés : un nœud défaillant n'engendre pas la panne dans tout le système. Néanmoins, dans ce genre de système, les nœuds ne collaborent pas entre eux pour atteindre un objectif commun en répartissant les calculs. Mais collaborent ensemble et parviennent à s'accorder sur leurs décisions à travers des protocoles de consensus, tout en évitant de se reposer sur un seul nœud qui centralise toutes les données et les calculs.

3 Définition de la technologie des registres distribués

Par définition, une technologie des registres distribués (DLT – Distributed Ledger Technology en anglais) est une base de données décentralisée manipulée par plusieurs nœuds dans un réseau décentralisé. La DLT est considérée comme la technologie mère de la blockchain. La structure de donnée qui gère et fait circuler l'information dans un tel réseau est appelée registre, où chaque nœud du réseau possède localement une copie de l'intégralité des informations contenues dans un registre. Chaque modification ou manipulation de l'information doit se faire simultanément et doit être validée par toutes les entités du réseau, ce qui donne la caractéristique d'immuabilité d'un tel réseau.

Contrairement à la blockchain, une information dans une DLT n'est pas validée grâce à un mécanisme de consensus, car ce dernier est très gourmand en termes de ressources, ce qui n'est pas pratique lorsqu'on a besoin d'une fluidité et d'une souplesse de notre réseau[48][49].

4 Qu'est-ce qu'une blockchain ?

La blockchain peut être vue comme l'héritière directe de la DLT, dont elle représente une évolution structurée et sécurisée. Alors que la DLT désigne tout système de registre distribué, la blockchain en est une implémentation spécifique qui organise les données en blocs liés de manière chronologique et sécurisés par des algorithmes cryptographiques et des mécanismes de consensus. Cette architecture garantit l'intégrité, la transparence et l'immutabilité des transactions, faisant de la blockchain un pilier des systèmes décentralisés modernes[48].

5 Consensus

Les protocoles de consensus permettent aux nœuds d'un réseau blockchain de s'accorder sur l'état des transactions, sans passer par une autorité centrale. Leur but est de garantir qu'une seule version de la chaîne de blocs est suivie par tous, assurant ainsi la sécurité et la fiabilité du système. Dans une organisation classique, les décisions sont prises par une seule personne ou un groupe restreint. En revanche, sur une blockchain, personne ne détient le pouvoir absolu. Ce sont les protocoles de consensus qui permettent aux participants de se mettre d'accord sur les transactions valides, même en présence d'acteurs malveillants ou défaillants[50][54].

6 Contrats intelligents

Les smart contracts, introduits par Nick Szabo au début des années 1990 [24], sont des programmes autonomes qui exécutent automatiquement des accords sur la blockchain. Ils garantissent la transparence et la sécurité en appliquant des règles prédéfinies. Un smart contract peut ajouter et lire des données, mais pas les modifier ni les supprimer, car la blockchain est immuable. Toute mise à jour crée un nouvel état des données. Dans Hyperledger Fabric, on parle de chaincodes. Contrairement aux smart contracts publics, les chaincodes fonctionnent dans un environnement privé et contrôlé, adapté aux blockchains de consortium. Ils définissent la logique métier et interagissent avec le registre distribué via une API, offrant flexibilité et contrôle[56].

7 Types de réseaux blockchain

Dans cette partie, nous allons pouvoir distinguer quatre types de blockchain qui sont utilisés aujourd'hui dans le monde des réseaux décentralisés :

7.1 Blockchain publique

Les deux premières générations blockchain, à savoir les blockchains 1.0 et 2.0, sont classées comme étant des blockchains dites publiques. Cela est dû au fait que n'importe quel utilisateur possédant une connexion internet peut rejoindre et participer à un réseau blockchain public tel que Bitcoin et Ethereum. Elles sont accessibles sans la moindre autorisation ; ainsi, chaque nœud du réseau peut lire, écrire et valider des transactions en suivant le ou les mécanismes de consensus du réseau. C'est pour cela qu, dans le jargon des réseaux blockchain, on fait référence à ce type de blockchain avec le mot "non-permissionné".

7.2 Blockchain privée

Une blockchain privée est une blockchain dont la création, la gestion et la modification sont prises en charge par une organisation privée[53], suivant sa propre modularité et adaptée à ses besoins. Dans ce type de blockchain, nous n'avons pas forcément besoin de cryptomonnaie pour la faire fonctionner, et seuls les membres (ou nœuds) autorisés peuvent accéder et valider les transactions. C'est pour cela qu'on parle de blockchain permissionnée pour définir ce type de réseau. Elles suivent une approche moins décentralisée que les blockchains publiques et adoptent des mécanismes de consensus plus souples et moins gourmands que ceux adoptés par Bitcoin ou Ethereum. Selon le Centre de droit bancaire et financier (CDBF), les blockchains

privées peuvent offrir une sécurité accrue pour des entreprises, notamment dans le secteur bancaire, ainsi que pour des institutions publiques[52]. L'exemple le plus connu dans ce type de blockchain est celui de Hyperledger Fabric développé et maintenu par IBM.

7.3 Blockchain de consortium

Une blockchain de consortium, appelée aussi blockchain fédérée, est un type de blockchain permissionné gouverné non seulement par une seule, mais par plusieurs organisations, dans le but de créer un réseau immuable et sécurisé entre celles-ci, ainsi que de partager les responsabilités de gestion, de manipulation et de maintenance du réseau. Elle combine à la fois des éléments des blockchains privées ainsi que ceux des blockchains publiques pour fonctionner. Ce type de réseau est idéal pour les chaines d'approvisionnement ainsi que le secteur bancaire, puisque les nœuds sont configurés pour gérer un réseau combiné par un groupe d'organisation plutôt qu'une seule entité comme dans une blockchain privée. Des exemples de blockchain fédérée peuvent être cités, tels que Energy Web Foundation ainsi QU'IBM FoodTrust [53][54][55].

7.4 Blockchain hybride

Une blockchain hybride est une combinaison des principes des blockchains publiques ainsi que de ceux des blockchains privées. Cette approche est idéale pour les organisations ou les entreprises qui veulent rendre une partie de leur réseau ou certaines informations publiques, tout en gardant un œil sur d'autres ressources ou données critiques en les rendant confidentielles. À titre d'exemple, on peut citer XinFin ainsi que Dragonchain qui illustrent bien le modèle des blockchains hybrides[53][54].

8 Domaines d'application de la blockchain

Initialement développée pour appuyer les cryptomonnaies, la technologie blockchain a vite prouvé son potentiel dans divers domaines en raison de ses propriétés essentielles comme la transparence, l'immutabilité, la capacité de suivi et la décentralisation. Elle est aujourd'hui considérée comme une solution novatrice pour traiter divers enjeux, allant de la gestion des informations confidentielles à l'amélioration des chaînes d'approvisionnement. Les exemples ci-dessous démontrent la variété des secteurs où la blockchain se révèle avoir une application pratique et prometteuse.

8.1 Internet des objets

On ne peut parler des applications de la blockchain sans invoquer sa complicité avec l'Internet des objets (IoT : Internet of Things, en anglais), car cette dernière est au cœur de la transformation numérique et de la modernisation du milieu industriel, notamment l'industrie manufacturière ainsi que les chaines d'approvisionnement, dans l'intention d'atteindre ce qu'on appelle l'industrie 4.0. Pour rappel, l'IoT se désigne par un ensemble de terminaux interconnectés à travers l'internet et qui sont dotés de capteurs, d'actionneurs, de programmes et/ou de logiciels leur permettant d'échanger des données entre eux, et ce dans un but bien précis : automatiser et smartiser la vie humaine. La blockchain, quant à elle, vient en complément à cette technologie pour lui donner une robustesse et une qualité supérieure en protection des données, tout en gardant la fluidité et la performance du réseau malgré la lourdeur des informations échangées [58][59].

8.2 Logistique et chaîne d'approvisionnement

La blockchain a un rôle crucial à jouer dans l'optimisation des chaînes d'approvisionnement, car elle offre une facilité de traçabilité des marchandises et la réduction des inefficacités administratives. Les registres distribués tiennent compte de chaque transaction de manière transparente, donnant donc une visibilité plus accrue sur le cycle de vie complet d'un produit. Cela aide à lutter contre la fraude, à améliorer la gestion des stocks et à automatiser les processus de contrôle au moyen des smart contracts [57].

8.3 Industrie manufacturière

Le déploiement de la blockchain dans les industries manufacturières simplifie davantage le traitement des ressources ainsi que l'automatisation de processus industriels. Elle permet la certification de la pièce et du produit ainsi que de garantir l'authenticité à l'aide de mécanismes de vérification basés sur des signatures cryptographiques. Elle facilite encore davantage la coopération entre les entreprises en permettant le partage sécurisé des données de production dans des réseaux de fabrication distribués[57].

9 Intégration de la blockchain dans les chaînes de production industrielles

La conversion digitale des systèmes industriels, en particulier dans le contexte de l'Industrie 4.0, souligne l'importance d'une traçabilité améliorée, d'une transparence plus grande et d'une protection des données à chaque étape du processus de production. Dotée d'attributs tels que l'immuabilité, la décentralisation et la transparence, la technologie blockchain constitue une réponse potentiellement efficace à ces besoins. En regroupant chaque transaction ou événement crucial de façon chronologique et inviolable, la blockchain assure la protection des données, depuis l'acquisition des matières premières jusqu'à la distribution du produit achevé.

Des recherches ont prouvé l'efficience de la blockchain pour optimiser les systèmes de gestion de la qualité (QMS) dans le secteur industriel. Par exemple, l'utilisation de la blockchain dans les procédures d'impression 3D assure un suivi intégral des paramètres de production, simplifiant par conséquent les audits et les vérifications de conformité [25]. En outre, la blockchain aide à diminuer les dangers associés à la falsification des données et à renforcer la transparence entre les divers intervenants de la chaîne logistique [26].

Hyperledger Fabric, considéré comme une plateforme blockchain permissionnée, se caractérise par sa modularité et sa faculté à établir des règles d'accès particulières pour chaque intervenant. Cette souplesse est particulièrement appropriée pour les contextes industriels où de nombreux acteurs collaborent sans nécessairement se faire confiance les uns aux autres. En offrant une gouvernance sur mesure et une gestion précise des identités, Hyperledger Fabric simplifie l'incorporation de la blockchain dans les systèmes actuels tout en adhérant aux exigences spécifiques de confidentialité et de performance du domaine industriel [19].

10 Hyperledger Fabric : architecture et éléments de base

Hyperledger est un projet open source, lancé en 2015 par la fondation LINUX, qui regroupe des frameworks, des outils et des bibliothèques dédiés à la création et au déploiement de blockchains privées et autorisées [37]. L'objectif principal de ce projet est de favoriser

l'utilisation de la blockchain permissionnée dans des contextes interorganisationnels et d'alléger la tâche des développeurs, en leur fournissant les instruments nécessaires pour élaborer, déployer et administrer des solutions blockchain adaptées aux environnements privés [38]. Hyperledger Fabric est la plateforme la plus utilisée et appréciée par les organisations, en raison de sa facilité d'utilisation et de son architecture modulaire qui offre un degré élevé de confidentialité, de résilience, de flexibilité et d'évolutivité [19]. Dans cette partie, nous allons explorer les composantes fondamentales qui forment un réseau blockchain basé sur Hyperledger Fabric.

10.1 Registre

Le registre distribué et immuable est la base de données de la blockchain. Il ne suit pas un format standard tel que les bases de données classiques, mais repose sur deux principes essentiels : l'immutabilité, qui garantit que les données ne peuvent pas être remodelées après avoir été enregistrées, et l'ordre chronologique, où les transactions sont ajoutées en fonction d'une séquence temporelle déterminée [39]. Grâce à ces caractéristiques, la blockchain assure la confiance, la transparence et la traçabilité des transactions [40].

Sous Hyperledger Fabric, le registre est composé de deux parties :

10.1.1 Journal des transactions

Le journal des transactions, parfois désigné comme base de données du registre (ledger database en anglais), est un fichier binaire où chaque nœud conserve une réplique localement, conservant ainsi la totalité de la chaîne de blocs apparue de manière séquentielle [41]. Du fait de son format amélioré pour assurer une performance optimale, il n'est pas directement accessible. Cependant, des outils ainsi qu'une API facilitent l'exploration des transactions et garantissent la réplication vers de nouveaux nœuds en cas de besoin [42].

10.1.2 Base de données de l'état global

La base de données de l'état global (world state database en anglais) est une spécificité d'Hyperledger Fabric. C'est une base de données classique qui est conservée localement sur chaque pair du réseau [22]. Elle illustre la situation présente de la blockchain à un moment précis, rendant l'accès aux informations plus simple sans avoir besoin d'examiner l'intégralité du registre [43]. Uniquement les pairs ayant obtenu une autorisation peuvent manipuler cette base de données. Quand un smart contract (chaincode) est exécuté et validé par le processus de consensus, l'état global est actualisé en fonction des règles établies par la gouvernance du réseau et des politiques de gestion des accès [19].

10.2 Noeuds d'ordre

Les nœuds d'ordre (Orderer en anglais) sont responsables de la structuration des transactions et de la création des blocs. Ils ne sont pas responsables de la validation des transactions, mais ils veillent à ce que toutes les entités du réseau voient les transactions dans un ordre cohérent [19]. Quand une série de transactions est présentée, les nœuds principaux les organisent en blocs et les transmettent à leurs homologues pour qu'ils soient enregistrés dans la blockchain. Ce mécanisme s'appuie sur un protocole de consensus tel que Raft, garantissant la résilience face aux défaillances et l'uniformité des informations au sein du

réseau [38]. Dans un environnement de production, on a souvent recours à plusieurs nœuds d'ordre pour assurer la continuité des services et renforcer la résilience.

10.3 Pairs

Les pairs sont des nœuds responsables de la conservation de la blockchain, de l'application des contrats intelligents et de la vérification des transactions [44]. On distingue deux types de pairs : les pairs qui endossent et les pairs qui valident [45]. Les validateurs pairs appliquent les contrats intelligents et authentifient les transactions selon la norme définie par le réseau. Une fois validées, les transactions sont transmises aux nœuds d'ordre pour être regroupées en un bloc [40]. D'autre part, les pairs validateurs ne sont pas responsables de la validation des transactions. Leur rôle est d'inscrire les blocs reçus et de mettre à jour l'état du registre. Chaque nœud conserve un registre contenant le journal des transactions et une base de données d'état global qui permet de suivre les mises à jour des données en temps réel.

10.4 Channels

Le canal est un dispositif permettant la création de sous-réseaux privés dans le réseau Hyperledger Fabric. Chaque canal offre la possibilité de regrouper un ensemble unique d'organisations capables d'émettre des transactions de manière distincte, indépendamment des autres membres [45]. Chaque canal possède un registre, des règles de gouvernance spécifiques et des contrats intelligents qui lui sont propres. Les canaux permettent de limiter l'accès aux informations, garantissant ainsi une confidentialité accrue des données. Un même pair peut faire partie de plusieurs canaux, ce qui lui offre la possibilité d'interagir avec divers sous-réseaux tout en préservant une distinction rigoureuse entre les données[46].

La figure II.1 montre l'architecture réseau Hyperledger Fabric, tout en mentionnant ses différents composants :

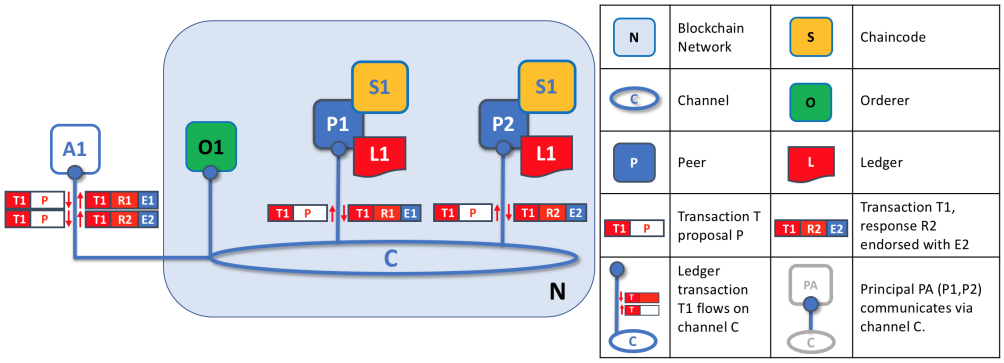

Figure II.1: Architecture générale d'un réseau Hyperledger Fabric[46]

10.5 Gestion des identités sous Hyperledger Fabric

Pour saisir comment les identités sont administrées dans Hyperledger Fabric, il est crucial de comprendre ce qu'est un fournisseur de service d'adhésion. Cependant, avant tout, nous devons comprendre deux aspects cruciaux : l'identité et l'autorité de certification Fabric CA[45].

10.5.1 Identité et Fabric CA

Dans le cadre d'une structure Hyperledger Fabric, une identité est attribuée, permettant ainsi l'authentification et l'obtention des droits nécessaires pour participer à un réseau. Ce certificat numérique X.509 [46], délivré par le Fabric CA qui joue le rôle d'autorité de certification au sein de la plateforme Hyperledger Fabric, représente en fait cette identité. Cette autorité de certification est un élément intégré dans l'ensemble des réseaux de cette catégorie et est administrée par le gestionnaire du réseau.

10.5.2 Membership Service Provider

Le Membership Service Provider(MSP), qui est présent sur chaque nœud orderer, peut parfois prêter à confusion. Il ne fournit pas d'autorisations ou de certificats aux participants du réseau, rôle qui est dévolu au Fabric CA. Son rôle principal est de confirmer les identités des participants, car il détient la liste des clés publiques de tous les participants. Cela permet de vérifier la signature numérique de chaque transaction et d'identifier l'origine de celle-ci [46].

10.6 Protocoles de consensus sous Hyperledger Fabric

Dans une blockchain, un protocole de consensus détermine les conditions selon lesquelles les nœuds s'accordent pour valider les blocs du réseau. Le réseau de blockchain publique Bitcoin utilise le protocole proof of work qui demande beaucoup de ressources pour réaliser des calculs complexes[46]. En revanche, sur le réseau Ethereum, on fait appel au proof of stake qui repose sur une mise de tokens pour augmenter les probabilités de sélection. Cependant, ces protocoles ne sont pas adaptés à un environnement privé comme celui des réseaux d'entreprise. C'est pourquoi Hyperledger Fabric propose des protocoles plus légers et faciles à déployer, tels que Raft, Kafka et Solo[47].

10.6.1 Solo

Le mode Solo est une méthode de fonctionnement très simple, exclusivement destinée au développement et aux tests. Il s'appuie sur un unique nœud d'ordre (orderer) qui valide et propage les transactions en l'absence de processus de consensus décentralisé. Comme il est vulnérable aux pannes et ne fournit pas de redondance, il n'est pas adapté à un environnement de production [45].

10.6.2 Kafka

Le protocole Kafka fait appel à un regroupement Kafka-ZooKeeper pour assurer la résilience face aux pannes et l'équilibrage des transactions [45]. Kafka fonctionne sur le principe du modèle de publication-abonnement (pub-sub), où un leader diffuse les blocs et les autres nœuds se chargent de les répliquer. Le protocole nous offre un consensus distribué et une résilience solide, mais nécessite une infrastructure complexe, ce qui a conduit les développeurs à le substituer par Raft [47].

10.6.3 Raft

Raft est désormais le système de consensus prédominant pour Hyperledger Fabric utilisé en production. Il opère sur la base d'un schéma leader-successeur, où un leader est désigné parmi les nœuds de commande (orderers) et a pour tâche d'organiser les transactions en blocs. Ces

blocs sont dupliqués par les autres nœuds qui en vérifient ensuite l'intégrité. Raft offre une résilience face aux défaillances, une meilleure capacité d'adaptation à la taille et évite le recours à des services externes comme Kafka/ZooKeeper, facilitant ainsi son déploiement et sa maintenance.

10.7 La sécurité des données sous Hyperledger Fabric

Quand on parle de technologie blockchain ou de DLT, on ne peut s'empêcher de reconnaitre leur finesse et leur supériorité en matière de sécurité et de protection des données contre la falsification. Et cela est dû au fait que ces technologies se reposent essentiellement sur des algorithmes de cryptographie connus pour leur robustesse. Sous Hyperledger Fabric, cette sécurité est renforcée grâce à la manière dont les blocs sont constitués. Chaque bloc regroupe un ensemble de transactions validées, auquel est associé un en-tête contenant notamment le hachage cryptographique du bloc précédent, assurant ainsi l'intégrité de la chaîne. Cette structure rend toute tentative de falsification pratiquement impossible sans compromettre l'ensemble des blocs suivants. Par ailleurs, chaque transaction est signée numériquement à travers l'identité du participant, garantissant l'authenticité et la non-répudiation des opérations. Ainsi, Hyperledger Fabric hérite non seulement des principes fondamentaux de la blockchain en matière de sécurité, mais les enrichit par une approche modulaire et rigoureuse adaptée aux environnements d'entreprise. La figure II.2 illustre la structure et l'enchainement des blocs dans un réseau Hyperledger Fabric.

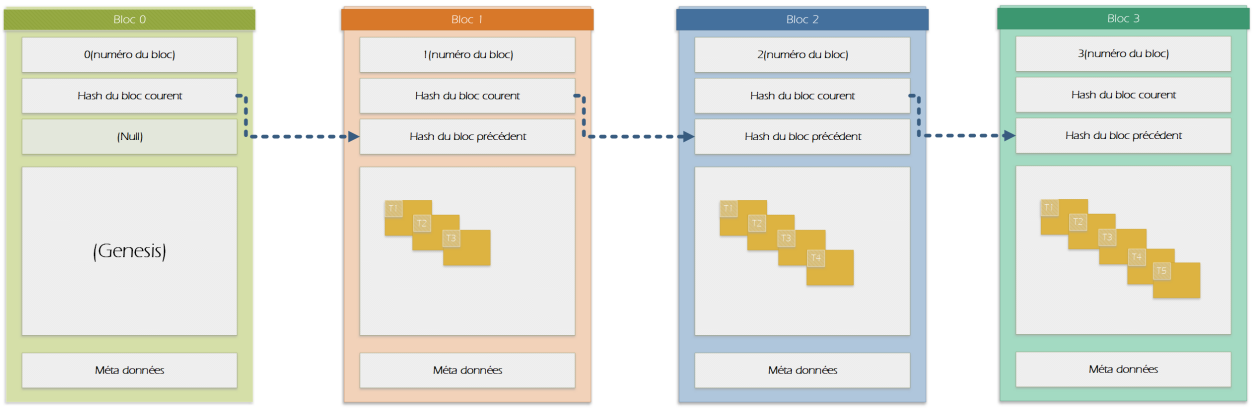

Figure II.2: structure et l'enchainement des blocs dans un réseau Hyperledger fabric.

10.8 Cycle de vie d'une transaction dans Hyperledger Fabric

Hyperledger Fabric opère selon un processus en trois phases : endorsement, ordering et validation. À l'opposé des blockchains traditionnelles où chaque nœud traite toutes les transactions, Fabric privilégie une méthode dénommée « Exécuter – Ordonner – Valider » qui améliore la performance et la confidentialité. Les phases d'une transaction se présentent comme suit [46]:

1. Une application cliente envoie une requête à un ou plusieurs endorsing peers, qui simulent l'exécution de la transaction à l'aide du chaincode.

2. Si les endorsing peers approuvent la transaction, ils renvoient une réponse signée à l'application.

3. L'application agrège ces réponses et envoie la transaction à l'ordering service, qui la place dans un bloc.

4. Le bloc est diffusé à tous les peers, qui procèdent à la validation (en vérifiant notamment les signatures et les conflits éventuels) avant d'ajouter le bloc au ledger.

La figure II.3 illustre le processus de déroulement d'une transaction sous Hyperledger Fabric, tel qu'expliqué ci-dessus :

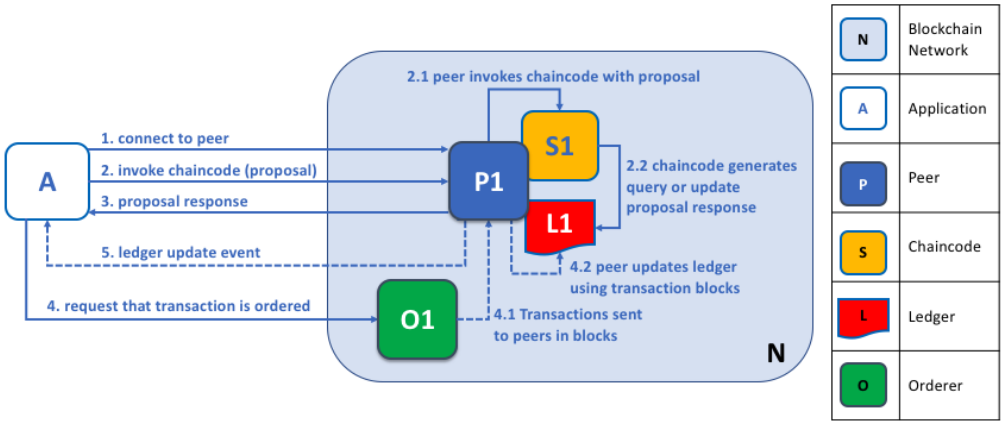

Figure II.3: Déroulement d'une transaction dans Hyperledger Fabric [37]

11 Performances et limites de Hyperledger Fabric dans les environnements industriels

Malgré la conception d'Hyperledger Fabric pour satisfaire les exigences des applications d'entreprise, diverses recherches ont souligné des problèmes liés à ses performances, particulièrement en ce qui concerne le taux de transactions et le délai de latence. Un examen détaillé a démontré que des éléments tels que la dimension des blocs, les politiques d'endossement et la sélection de la base de données d'état ont un impact notable sur l'efficacité du réseau [22]. Par exemple, l'emploi de CouchDB en tant que base de données d'état pourrait engendrer des délais supplémentaires lors de la vérification des transactions.

Des études ont suggéré des améliorations pour optimiser les performances de Hyperledger Fabric. Parmi ces améliorations, la réalisation simultanée des contrôles d'endossement, l'enregistrement en mémoire tampon des identités et l'amélioration des opérations de lecture et d'écriture ont contribué à accroître le volume des transactions tout en diminuant la latence [27]. Par ailleurs, l'utilisation de réseaux de Petri stochastiques pour modéliser les performances a permis d'obtenir une meilleure compréhension des points de congestion et des moyens pour les réduire [28].

Il est également essentiel de souligner que les performances sont directement influencées par la configuration du réseau, y compris le nombre de pairs et le volume des transactions. Des recherches ont démontré que l'augmentation de la quantité de pairs pourrait renforcer la résistance aux défaillances, tout en instaurant une complexité additionnelle et une utilisation intensifiée des ressources [28].

12 Cas pratiques de l'utilisation de Hyperledger Fabric

De nombreux projets majeurs ont illustré la capacité de Hyperledger Fabric à révolutionner les chaînes d'approvisionnement, à optimiser la traçabilité et à renforcer la confiance entre les différents intervenants du secteur industriel. Même si leur présence dans le secteur de la fabrication proprement dit reste limitée, ces exemples concrets, majoritairement tirés du domaine agroalimentaire, offrent des leçons cruciales pour envisager une utilisation plus étendue [30].

Le projet IBM Food Trust figure parmi les initiatives les plus marquantes et occupe une position centrale. Ce réseau blockchain, élaboré en collaboration avec IBM, offre aux intervenants du secteur agroalimentaire (producteurs, distributeurs, détaillants) la possibilité de tracer les produits à chaque phase du processus logistique. Avec Hyperledger Fabric, les données concernant l'origine, la qualité et les conditions de transport sont gravées de façon inaltérable et mises en commun entre les participants autorisés [31].

Walmart, un pionnier dans ce secteur, a dirigé plusieurs initiatives pilotes de traçabilité en utilisant Hyperledger Fabric[34]. Un des résultats les plus marquants est la notable diminution du temps requis pour tracer l'origine d'un produit : alors qu'auparavant, déterminer la provenance exacte d'un lot de mangues aux États-Unis pouvait prendre plusieurs semaines, l'utilisation de la blockchain a permis de réduire ce laps de temps à quelques secondes seulement [24]. Cette vitesse améliorée offre non seulement une réduction des pertes économiques lors d'une crise sanitaire, mais contribue également à renforcer la sécurité alimentaire et la confiance des consommateurs.

Carrefour a également été actif en Europe, en incorporant Hyperledger Fabric dans son système de traçabilité des aliments. Le client a la possibilité, en balayant un simple QR code sur un article, d'accéder à tout l'historique du produit : lieu et date de fabrication, détails sur l'éleveur ou le producteur, parcours logistiques, accréditations obtenues, etc. Cette sorte d'initiative démontre que Hyperledger Fabric peut occuper une position clé dans la mise en valeur des produits, en satisfaisant les exigences récentes des consommateurs relatives à la transparence et à la durabilité [32].

Actuellement, plusieurs domaines étudient l'implémentation de Hyperledger Fabric pour optimiser la qualité des processus industriels : suivi des composants, validation des phases de production, automatisation des vérifications qualité par le biais de contrats intelligents. Cependant, la majorité de ces initiatives demeure au stade de prototype ou de projet pilote. Cela met en évidence le besoin constant de recherches et d'expérimentations afin de confirmer intégralement les avantages de cette technologie dans des environnements manufacturiers plus étendus [33].

13 Lean Six Sigma et Hyperledger Fabric : une synergie autour de la qualité, des coûts et du temps

Le Lean Six Sigma (LSS), très répandu dans le secteur de la fabrication, se concentre sur l'amélioration continue des processus en minimisant les déchets, les défauts et les fluctuations, en se basant sur trois aspects essentiels : la qualité, les coûts et le délai. L'usage de la technologie blockchain, notamment via la plateforme Hyperledger Fabric, offre des opportunités inédites pour améliorer ces aspects cruciaux.

En termes de qualité, Hyperledger Fabric propose un cadre technique qui assure l'intégrité, la transparence et la traçabilité des données. Chaque événement ou action associée à un processus industriel peut être inscrit de manière inaltérable et horodatée dans le registre

distribué, empêchant ainsi les falsifications, assurant la vérification des historiques de production et fournissant une fondation solide pour les analyses statistiques et les décisions dans le contexte des projets Six Sigma [35]. De plus, l'usage de contrats intelligents permet d'automatiser les contrôles qualité en intégrant directement les règles de conformité dans le système, ce qui favorise une détection précoce des anomalies et une meilleure réactivité face aux défauts [36].

En termes de coûts, l'automatisation des processus de vérification et de validation via la blockchain entraîne une diminution notable des dépenses associées aux contrôles manuels, aux audits sur papier et aux fautes de saisie. Puisque les données sont protégées dès leur création et partagées de façon régulée entre les intervenants, on évite la duplication, on diminue les conflits et on utilise plus efficacement les ressources. Ceci est parfaitement aligné avec la philosophie Lean, qui cherche à supprimer les actions sans valeur ajoutée tout en optimisant l'efficacité globale [35].

Enfin, sur le plan temporel, Hyperledger Fabric facilite l'accélération des processus de prise de décision et opérationnels en fournissant immédiatement des données fiables et en permettant une validation rapide des transactions. La blockchain, à l'opposé des méthodes centralisées nécessitant plusieurs étapes de validation asynchrones, permet une mise à jour presque immédiate des registres pour toutes les entités autorisées. Cette souplesse diminue les délais de production, perfectionne la coordination entre les phases de fabrication et amplifie l'agilité générale du système industriel. Il a été démontré que des améliorations dans la configuration de Fabric peuvent considérablement augmenter le volume des transactions tout en diminuant la latence, rendant ainsi cette technologie applicable même dans les processus soumis à des contraintes de temps strictes [22].

Par conséquent, l'incorporation de Hyperledger Fabric dans les initiatives Lean Six Sigma représente un progrès stratégique pour les entreprises industrielles souhaitant renforcer la qualité de leurs procédures, contrôler leurs dépenses et améliorer leur réactivité. Elle associe les principes solides du LSS aux garanties technologiques de la blockchain, proposant ainsi une approche innovante et plus résistante de la gestion de la performance industrielle.

14 Conclusion

L'étude des écrits confirme que la blockchain, plus précisément Hyperledger Fabric, présente des possibilités réelles pour renforcer la traçabilité, la transparence et la sûreté dans les chaînes de production industrielles. Son architecture autorisée, sa capacité de modularité et son intégration flexible en font une option appropriée pour les milieux de fabrication complexes.

Les études recensées démontrent qu'Hyperledger Fabric est capable de satisfaire aux besoins industriels, bien qu'il existe des contraintes techniques relatives à la performance. Ces limitations, particulièrement concernant la latence et la résolution de conflits, sont actuellement en cours d'optimisation dans le cadre des recherches actuelles.

Les exemples concrets relevés, en particulier dans le domaine de l'agroalimentaire, démontrent l'intérêt de Fabric pour des utilisations pratiques, tout en préparant le terrain pour une adoption plus étendue dans divers autres domaines. De plus, son incorporation aux processus Lean Six Sigma démontre qu'elle a le potentiel de consolider les initiatives d'amélioration continue en appuyant les trois fondements que sont la qualité, les coûts et les délais.

Cet état de l'art établit donc les fondements d'une analyse approfondie des méthodes concrètes d'application de la blockchain dans un contexte industriel et guide les futurs travaux vers une expérimentation spécifique ou une suggestion d'architecture sur mesure.

Chapter III

Proposition d'une solution basée sur Hyperledger Fabric

1 Introduction

Le secteur industriel occupe une place centrale dans l'économie moderne, jouant un rôle clé dans la transformation des matières premières en produits finis destinés à la consommation ou à d'autres industries. Il s'appuie sur des chaînes de production complexes, souvent automatisées, qui impliquent de nombreux équipements, intervenants et processus interconnectés.

Avec l'évolution des technologies numériques, l'industrie connaît aujourd'hui une transformation profonde appelée Industrie 4.0, caractérisée par l'intégration de technologies telles que l'Internet des Objets (IoT), l'intelligence artificielle, l'analyse de données à grande échelle (Big Data) et la blockchain. Cette transition vise à rendre les systèmes de production plus intelligents, efficaces, flexibles et sécurisés.

Dans ce contexte, la gestion des données industrielles devient un enjeu crucial. Les processus de production génèrent une quantité importante d'informations, qu'il s'agisse de données liées aux matières premières, aux étapes de fabrication, à la maintenance des équipements ou encore à la qualité des produits finis. Ces données doivent être collectées, traitées, stockées et exploitées de manière fiable afin d'optimiser la performance industrielle, mais aussi d'assurer une traçabilité complète et transparente des opérations.

C'est dans cette dynamique de transformation numérique que s'inscrit l'objectif de ce stage : explorer l'intégration de la technologie blockchain au sein d'un environnement industriel réel pour renforcer la traçabilité et l'intégrité des données tout au long de la chaîne de production.

2 Problèmatique

Dans une chaîne de production industrielle, la maîtrise et la fiabilité des informations sont essentielles pour garantir une gestion efficace des processus, une qualité constante des produits ainsi qu'une traçabilité complète de chaque étape. Toutefois, dans de nombreuses entreprises, ces informations sont souvent fragmentées, stockées de manière centralisée ou manuellement enregistrées, ce qui entraîne plusieurs difficultés majeures :

- Un manque de transparence dans les processus, rendant difficile la vérification rapide de l'origine et de l'état des produits à un instant donné.

- Une traçabilité limitée, notamment lorsqu'il s'agit de reconstituer l'historique d'un produit ou d'identifier l'origine d'un défaut.
- Une vulnérabilité aux erreurs humaines ou aux modifications non autorisées des données, pouvant nuire à l'intégrité des informations.
- Une dépendance à des systèmes internes ou à des bases de données centralisées, exposées aux pannes ou aux attaques informatiques.

Dans un contexte où la réactivité, la qualité, et la conformité aux normes sont des enjeux cruciaux, ces limites peuvent compromettre la compétitivité de l'entreprise. C'est dans ce cadre que se pose la question suivante :

Comment améliorer la traçabilité, la fiabilité et l'intégrité des données dans une chaîne de production industrielle, tout en assurant un accès rapide et sécurisé à l'information ?

La blockchain, en tant que registre distribué, transparent et immuable, apporte une réponse innovante à cette problématique. En enregistrant les données de manière décentralisée, infalsifiable et horodatée, elle permet de suivre chaque événement de production, de valider les opérations sans tiers de confiance et de renforcer la transparence du processus industriel.

C'est dans ce cadre que s'inscrit ce travail, dont l'objectif est d'étudier et d'expérimenter l'intégration de la blockchain Hyperledger Fabric dans un cas concret de production industrielle, au sein de SARL Ibrahim et Fils - Ifri.

3 Présentation de l'entreprise d'accueil : SARL Ibrahim et Fils - Ifri

La SARL Ibrahim et Fils, plus connue sous sa marque Ifri, est une entreprise algérienne spécialisée dans la production et la commercialisation d'eaux minérales naturelles et de boissons diverses. Fondée en 1993, l'entreprise est implantée dans la wilaya de Béjaïa, plus précisément dans la région d'Ighzer Amokrane, réputée pour la qualité exceptionnelle de ses sources d'eau.

Ifri s'est imposée comme l'un des leaders du marché national grâce à un positionnement axé sur la qualité, l'innovation, et le respect des normes sanitaires internationales. Elle dispose de plusieurs lignes de production modernes, automatisées et capables de répondre à une demande croissante, tout en assurant une hygiène et une sécurité irréprochables.

Son produit phare, l'eau minérale naturelle Ifri, est puisée directement à la source et embouteillée sans subir de traitement chimique, ce qui lui permet de conserver toutes ses propriétés naturelles. En plus de l'eau, l'entreprise propose une large gamme de boissons gazeuses, jus et eaux aromatisées, destinées aussi bien au marché national qu'à l'export.

Dans une perspective de modernisation et dans le cadre d'une transition progressive vers les principes de l'Industrie 4.0, il serait pertinent pour l'entreprise Ifri d'envisager l'intégration de technologies innovantes telles que l'Internet des Objets (IoT), l'automatisation avancée, et plus récemment, la blockchain. Ces outils pourraient permettre d'optimiser les processus internes, en particulier ceux liés à la traçabilité de la production et à la sécurisation des

données industrielles, tout en améliorant la transparence et la réactivité du système de production.

4 Description de la solution proposée

La solution proposée repose sur l'enregistrement systématique des transactions liées aux palettes tout au long de leur cycle de vie, via un réseau blockchain Hyperledger Fabric. Chaque étape, de la réception des matières premières à l'expédition du produit final, est tracée de manière fiable, immuable et sécurisée.

L'utilisation de smart contracts permet de garantir à la fois l'intégrité des données et l'automatisation des validations, sans intervention humaine. De plus, la mise en œuvre de canaux privés (private channels) assure la confidentialité des échanges entre les différents services internes de l'usine.

Les principaux acteurs internes concernés par ce système sont :

- **L'entrepôt des matières premières :** chargé de la réception et du stockage des matériaux nécessaires à la production des bouteilles d'eau.
- **La chaîne de fabrication :** où les matières premières sont transformées et conditionnées.
- **L'entrepôt des produits finis :** qui gère le stockage et la préparation des palettes pour la distribution.

Les figures III.1 et III.2 mettent en évidence les interactions entre les différents composants du réseau, ainsi que la manière dont les informations sont capturées et inscrites dans la blockchain.

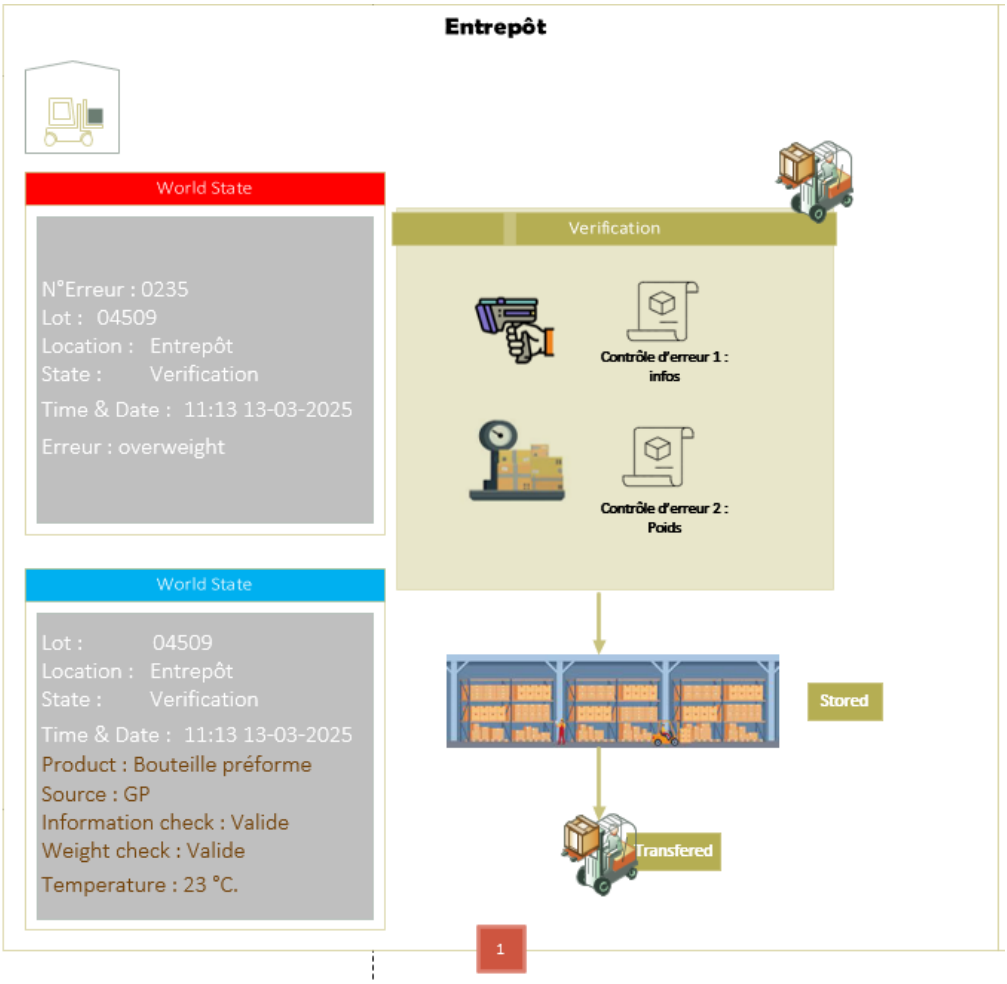

Figure III.1: Illustration du processus d'enregistrement dans l'entrepôt des matières premières

La figure III.1 représente le processus standard d'un entrepôt, qu'il soit consacré aux matières premières ou aux produits finis, car ils obéissent à une logique comparable. Lors de l'arrivée d'une palette, un contrôle d'intégrité des données est réalisé afin de s'assurer de la exactitude des informations liées. Puis, un contrôle du poids est effectué pour identifier toute irrégularité potentielle. Après avoir traversé ces étapes, la palette est entreposée en attendant de poursuivre son parcours vers une autre phase du processus industriel. Toutes les données concernant ces opérations sont inscrites dans le premier registre, assurant une traçabilité intégrale de chaque lot. Si une anomalie est identifiée, comme un poids incorrect ou des données absentes, une entrée est automatiquement insérée dans le second registre consacré aux erreurs, précisant la nature du problème, son emplacement et le moment où il a été détecté.

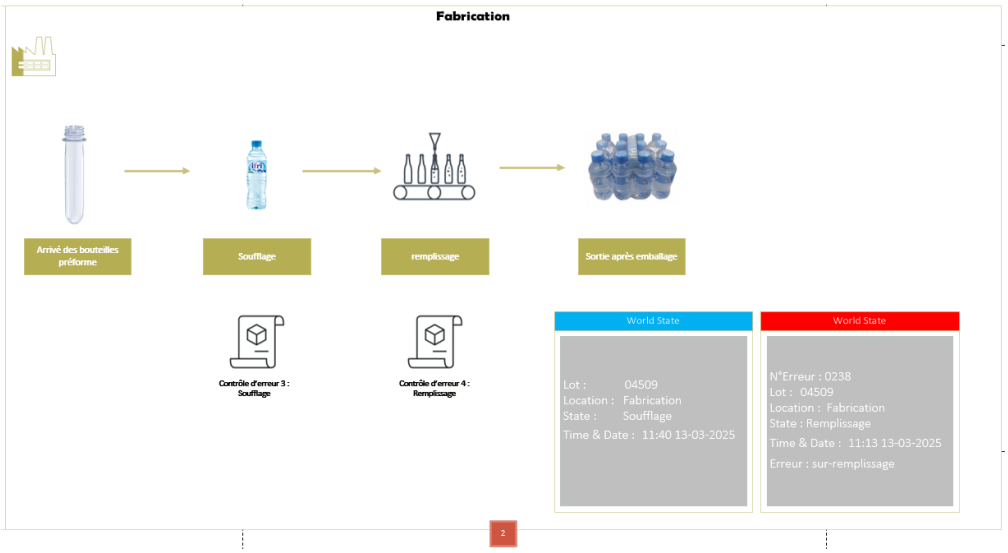

Figure III.2: Enregistrement des données tout au long du processus de fabrication

La figure III.2 présente le processus des opérations à travers la chaîne de production. Une fois arrivées depuis l'entrepôt, les bouteilles préformes passent par un processus de soufflage pour acquérir leur forme finale. Une première vérification de la conformité est effectuée pour repérer les imperfections liées au soufflage. Les bouteilles qui répondent aux critères sont ensuite soumises à la phase de remplissage avec de l'eau minérale. Une seconde vérification est ensuite effectuée pour s'assurer que la volume d'eau dans chaque bouteille se situe dans le cadre permis de 0,48L à 0,52L. Si une bouteille excède ou ne respecte pas cette plage, l'anomalie est aussitôt consignée dans le second registre, qui regroupe toutes les erreurs identifiées dans le système. Ce système de repérage et d'enregistrement des irrégularités, associé à la traçabilité fournie par le premier registre, contribue à améliorer le contrôle qualité et la transparence de l'ensemble du processus de production.

5 Mise en œuvre de la solution

Dans cette section, nous détaillons la mise en œuvre technique de la solution basée sur Hyperledger Fabric. Nous commencerons par décrire l'architecture du réseau, qui repose sur la séparation des données en deux canaux distincts pour une meilleure gestion et une sécurité accrue. Ensuite, nous expliquerons la structure des registres (ledgers), chacun étant associé à un canal, et leur rôle dans le processus de suivi et de gestion des erreurs.

6 Architecture du réseau et enregistrement des données

Le réseau Hyperledger Fabric mis en place repose sur deux canaux distincts, chacun possédant son propre registre (ledger). Cette approche favorise une séparation logique des données, améliore la gestion des droits d'accès et renforce la confidentialité des échanges.

- **Le premier canal** est dédié à la traçabilité des palettes. Il enregistre toutes les transactions depuis la réception des matières premières jusqu'à l'expédition des produits finis. Ce registre centralise les données liées aux étapes de fabrication, au suivi des composants ainsi qu'au contrôle qualité. Ce canal peut être partagé entre différentes organisations ou départements impliqués dans la chaîne de production.

- **Le second canal** est spécifiquement conçu pour la gestion des anomalies. Il permet d'enregistrer les événements inhabituels, les incidents techniques etles non-conformités détectées en production.

Cette séparation permet une analyse ciblée des erreurs tout en maintenant l'intégrité du registre principal. La figure III.3 résume l'architecture du réseau Hyperledger Fabric mis en place, illustrant les deux canaux et les interactions entre les différents composants.

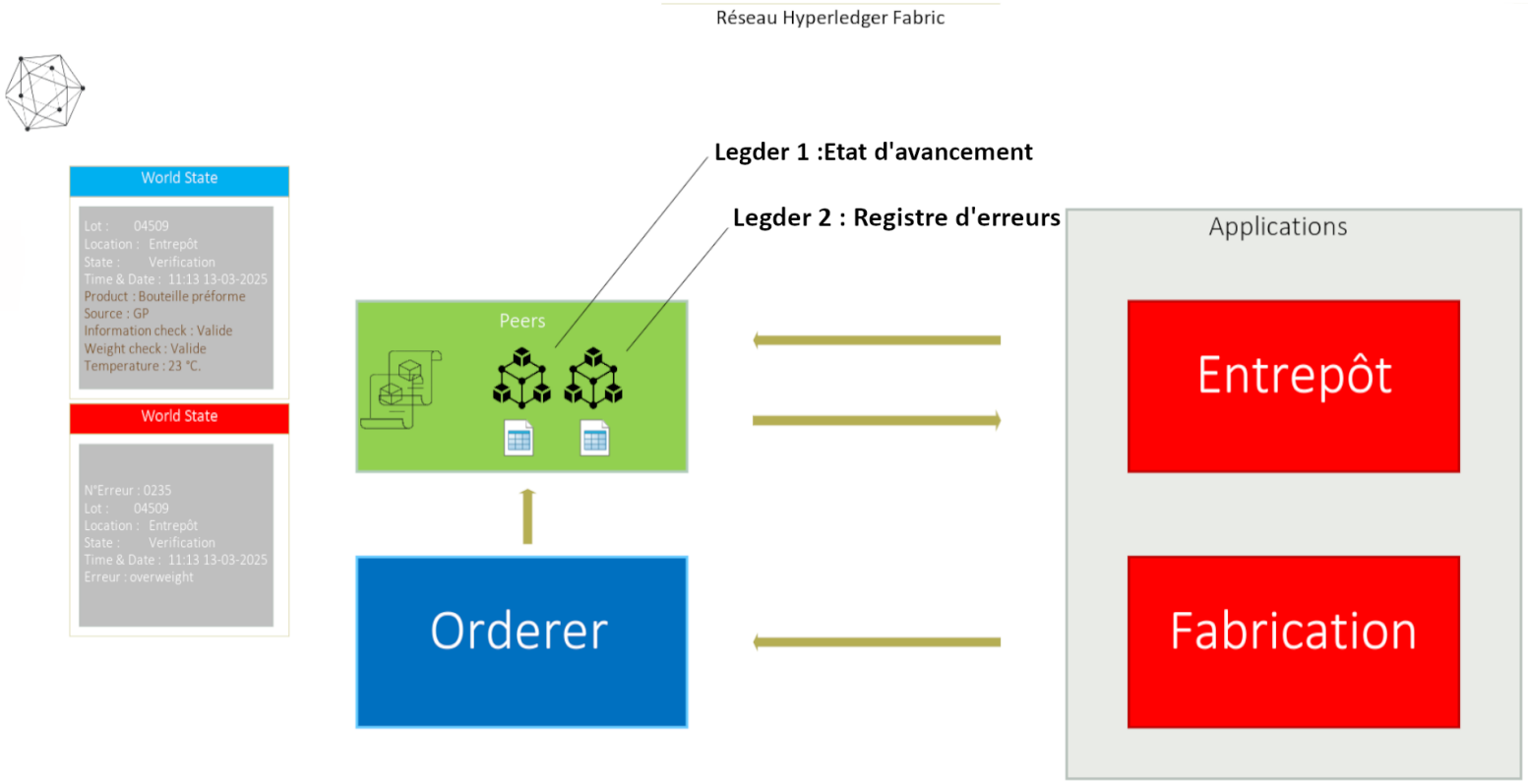

Figure III.3: Vue d'ensemble du réseau Hyperledger Fabric dans le système de production d'eau minérale

7 Contenu des registres (ledgers)

Afin d'assurer une structuration précise et exploitable des données, chaque ledger contient un ensemble de champs spécifiques à son objectif.

Ledger 1 - Suivi de la production et traçabilité des palettes :

Champ	Description
N°Lot	Numéro unique identifiant le lot de production
Location	Emplacement actuel : entrepôt ou ligne de fabrication
State	État du lot (ex. : réceptionné, en cours de traitement, vérifié, etc.)
Time/Date	Date et heure de l'enregistrement
Product	Type de produit (ex. : eau minérale 0.5L, 1.5L, etc.)
Source	Origine de l'entrée (entrepôt de matières premières, unité de production...)
Information check	Validation des données saisies (valide / non valide)
Weight check	Résultat du contrôle de poids (valide / non valide)
Temperature	Température mesurée (applicable uniquement dans l'entrepôt)

Ledger 2 - Gestion des anomalies et erreurs de production :

Champ	Description
N°Error	Identifiant unique de l'anomalie
Lot	Numéro du lot concerné
Location	Emplacement où l'erreur a été détectée
State	État au moment de l'anomalie (ex. : en inspection, rejeté)
Time & Date	Date et heure de l'incident
Erreur	Type d'anomalie détectée (ex. : surcharge, fuite, etc.)

8 Gestion des Smart Contracts dans la Traçabilité des Processus de Production

Les smart contracts jouent un rôle central dans la gestion des processus de production en automatisant la vérification et la validation des données tout au long de la chaîne de production. Sous Hyperledger Fabric, ces contrats permettent de garantir l'intégrité des informations et d'assurer la traçabilité des opérations, tout en favorisant l'efficacité en éliminant la nécessité d'interventions manuelles.

8.1 Objectif des Smart Contracts

Dans le cadre de la production des bouteilles d'eau chez SARL Ibrahim et Fils - Ifri, plusieurs smart contracts sont mis en œuvre afin de contrôler la conformité des différentes étapes de la production. Ces smart contracts sont déployés sur le réseau Hyperledger Fabric, chacun étant associé à un des canaux privés du réseau. L'objectif principal est d'automatiser les contrôles qualité et d'enregistrer les erreurs détectées, tout en assurant la transparence et la sécurité des informations grâce à l'immuabilité du registre blockchain.

8.2 Smart Contract 1 : Vérification des Informations et du Poids des Palettes

Le premier smart contract intervient lors de la réception des palettes dans l'entrepôt. Il permet de vérifier l'intégrité des informations de la palette ainsi que son poids, afin de garantir la conformité avant son introduction dans la chaîne de production. **Déroulement du Smart Contract 1 :**

1. **Réception des palettes :** Chaque palette est scannée à l'aide d'un dispositif RFID, et les informations relatives à la palette (comme le numéro de lot, le type de produit, etc.) ainsi que son poids sont extraites.

2. **Vérification des informations :** Le smart contract vérifie l'intégrité des informations extraites. Toute information manquante ou erronée entraîne l'annulation de l'action et l'enregistrement de l'erreur dans le ledger des anomalies.

3. **Vérification du poids :** Le poids de la palette est comparé au poids attendu pour le lot. Si le poids est hors de la plage attendue, l'action est annulée et l'anomalie est enregistrée.

4. **Enregistrement de la transaction :** Si toutes les conditions sont remplies, la palette est autorisée à passer à l'étape suivante de production. Sinon, elle est mise en quarantaine, et un rapport d'erreur est généré dans le ledger des anomalies.

Le smart contract s'assure ainsi que seules les palettes conformes sont introduites dans le processus de fabrication, renforçant ainsi la qualité de la production et la sécurité des données.

Le flowchart ci-après synthétise le fonctionnement de ce smart contract dédié au contrôle des palettes dans l'entrepot.

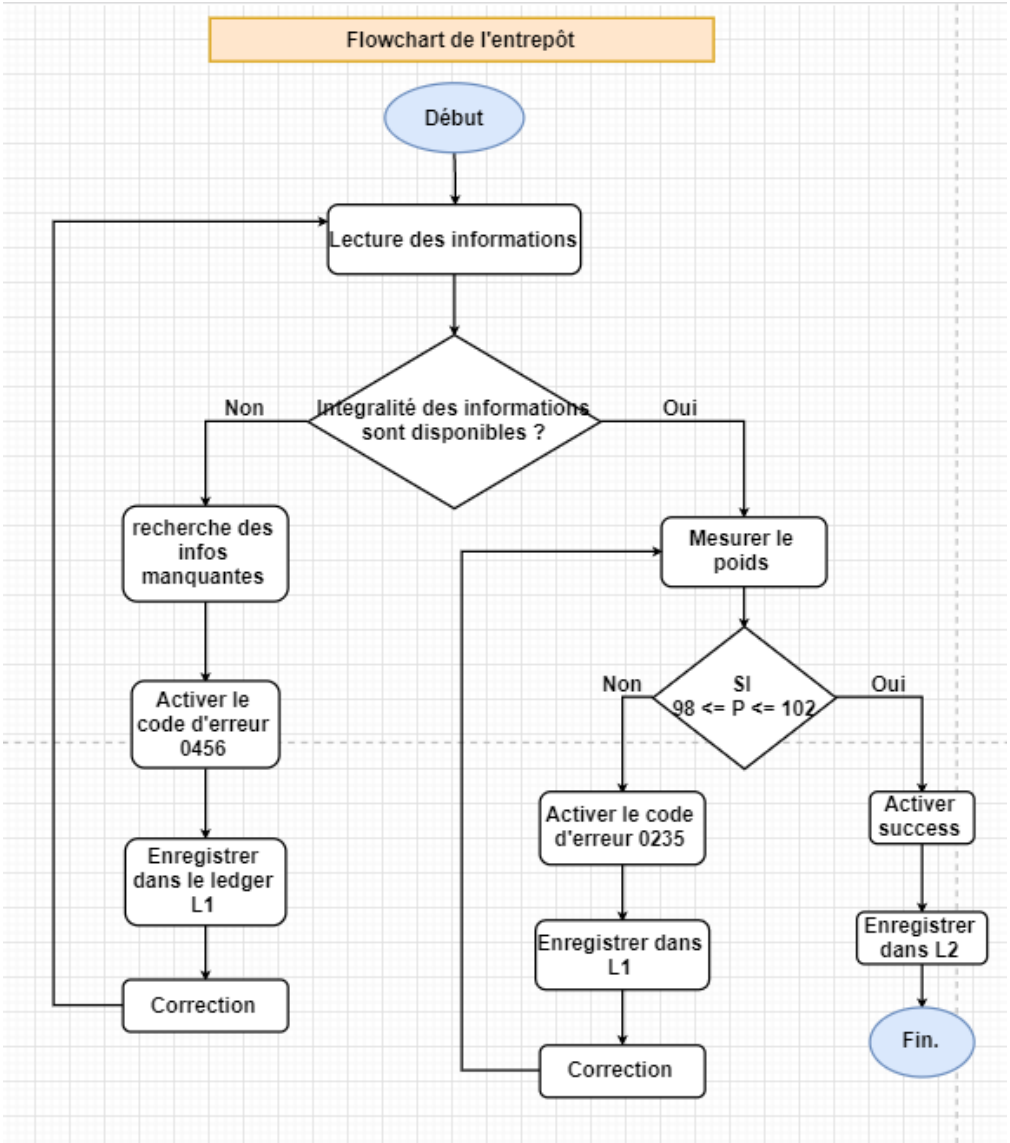

Figure III.4: Flowchart illustrant le fonctionnement du chaincode dédié au contrôle des palettes dans l'entrepot

8.3 Smart Contract 2 : Vérification du Soufflage des Bouteilles

Le deuxième smart contract est mis en œuvre après le processus de soufflage des bouteilles. Il vérifie la qualité du soufflage et détecte les éventuelles anomalies liées à la formation des bouteilles.

Processus du Smart Contract 2 :

1. **Arrivée des préformes :** Les bouteilles préformes sont envoyées à la souffleuse pour être transformées en bouteilles.

2. **Soufflage des bouteilles :** Chaque bouteille est formée à l'issue du processus de soufflage.

3. **Vérification de la qualité du soufflage :** Si une bouteille présente une anomalie (par exemple, une déformation ou une mauvaise forme), l'erreur est détectée et enregistrée dans le ledger des anomalies.

4. **Enregistrement de la transaction :** Les bouteilles soufflées correctement sont validées et enregistrées dans le ledger de traçabilité de la production. Celles présentant une anomalie sont mises en quarantaine et un rapport d'erreur est généré dans le ledger des anomalies.

Ce smart contract garantit que seules les bouteilles correctement soufflées sont validées et poursuivent leur chemin dans le processus de production. Le flowchart ci-après synthétise le fonctionnement de ce smart contract dédié au contrôle du processus de soufflage.

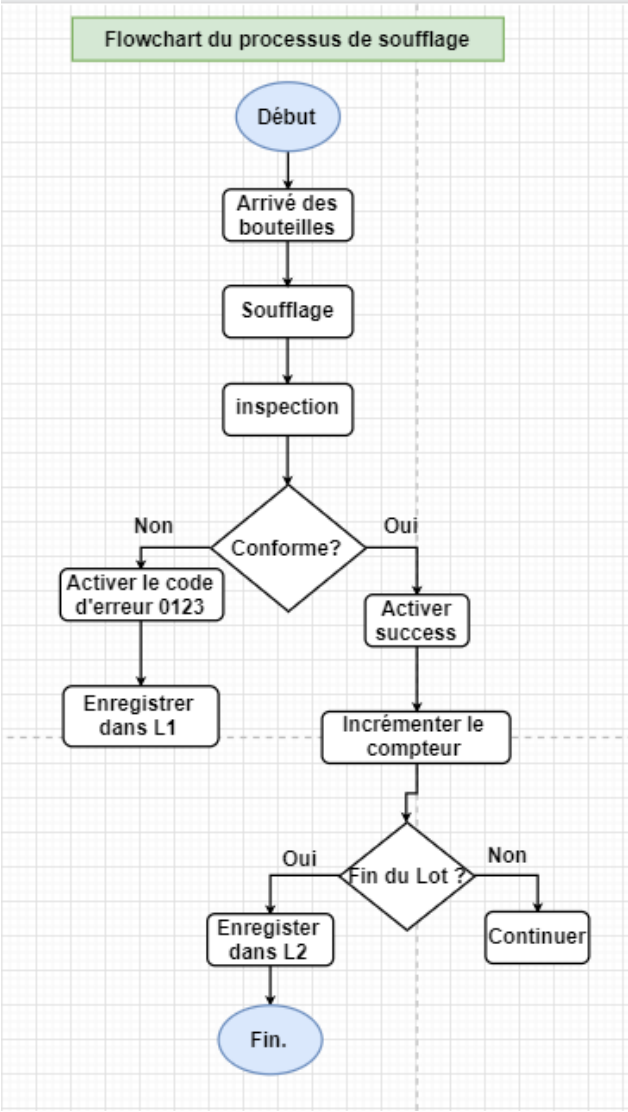

Figure III.5: Flowchart illustrant le fonctionnement du chaincode dédié au contrôle du processus de soufflage

8.4 Smart Contract 3 : Vérification du Remplissage des Bouteilles

Le troisième smart contract est implémenté pour garantir que chaque bouteille est remplie dans les normes de volume spécifiques (0,48L à 0,52L pour une bouteille de 0,5L). Ce contrat détecte les anomalies de remplissage, telles que les bouteilles sous-remplies ou sur-remplies.

Processus du Smart Contract 3 :

1. **Remplissage des bouteilles :** Les bouteilles soufflées et prêtes à être remplies sont envoyées à l'unité de remplissage.

2. **Vérification du volume :** Le smart contract vérifie que le volume de liquide contenu dans chaque bouteille se situe dans la plage acceptée, soit entre 0,48L et 0,52L.

3. **Validation du remplissage :** Si la bouteille respecte la norme de volume, elle est validée et enregistrée dans le ledger de production. Si elle est mal remplie, une erreur est générée.

4. **Enregistrement de la transaction :** Les bouteilles conformes sont envoyées à l'étape suivante, tandis que celles avec des erreurs sont mises de côté pour inspection manuelle, et un rapport d'erreur est enregistré dans le ledger des anomalies.

Ce smart contract assure le respect des spécifications de remplissage pour chaque bouteille, garantissant ainsi la qualité du produit final. Le flowchart ci-après synthétise le fonctionnement de ce smart contract dédié au contrôle du remplissage.

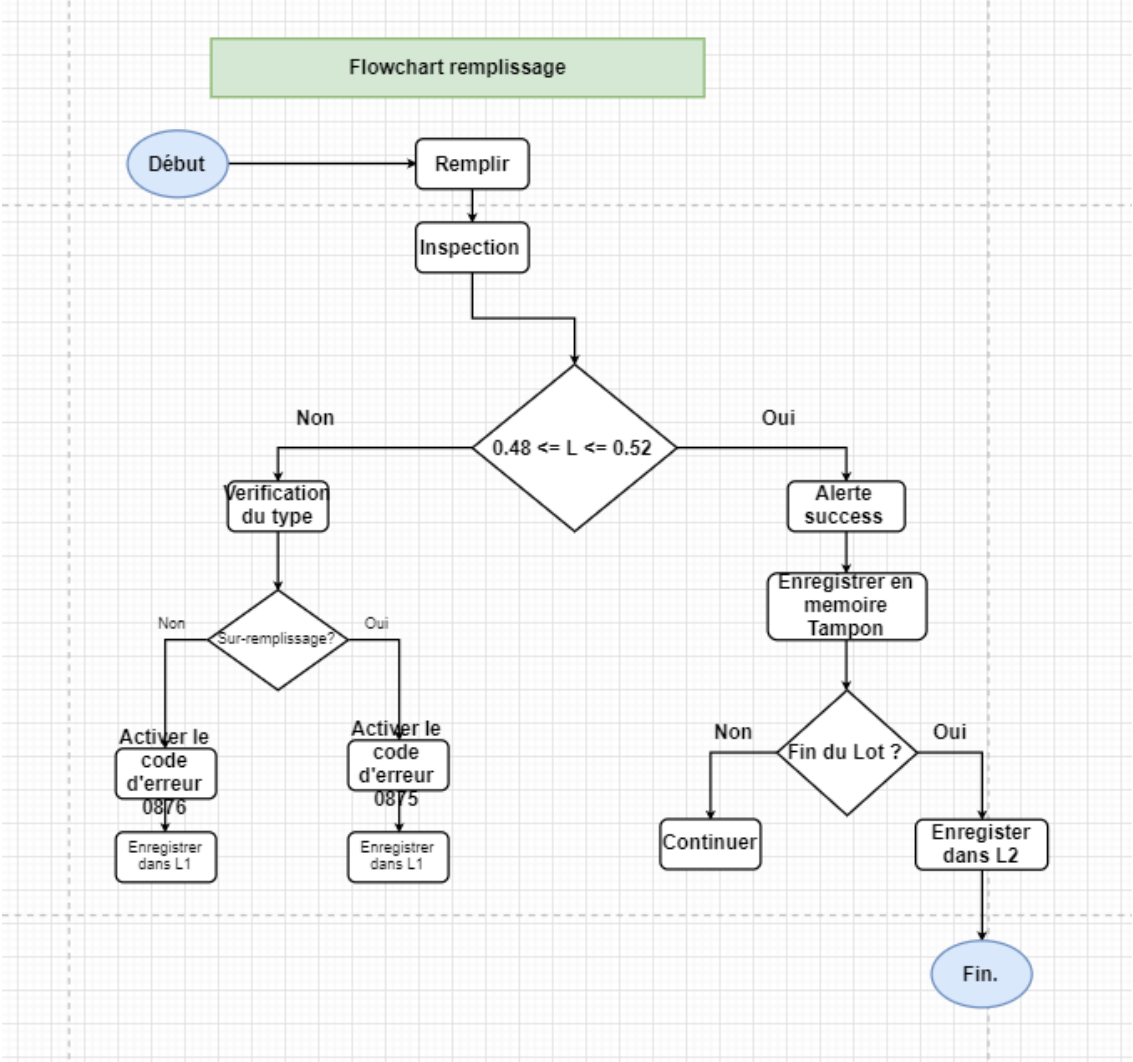

Figure III.6: Flowchart illustrant le fonctionnement du chaincode dédié au contrôle du processus du remplissage

9 Sécurité et gestion des accès

Dans une architecture distribuée comme celle de Hyperledger Fabric, la sécurité et le contrôle des accès sont des éléments fondamentaux. Chaque participant du réseau est authentifié à l'aide de certificats numériques X.509 délivrés par un Certificate Authority (CA) intégré au système. Ces certificats permettent de vérifier l'identité de chaque utilisateur et de contrôler l'accès aux ressources du réseau.

Le Membership Service Provider (MSP) joue un rôle clé dans la gestion des identités et des permissions. Il permet d'attribuer des rôles spécifiques aux différents acteurs (administrateurs, utilisateurs, applications clientes), garantissant ainsi que seules les entités autorisées peuvent soumettre ou valider des transactions, accéder à certains canaux ou exécuter des smart contracts.

Cette approche assure une confidentialité des échanges, une intégrité des opérations, et une traçabilité complète des actions réalisées sur le réseau.

10 Implémentation Complète de la Solution

L'implémentation de la solution blockchain dédiée à la traçabilité des lots d'eau dans un environnement industriel a été conduite selon une démarche méthodique articulée en plusieurs phases distinctes. Chaque phase a été rigoureusement validée avant de passer à la suivante, afin de garantir la stabilité, la reproductibilité et la robustesse du système final. Le déploiement s'est appuyé sur la technologie Hyperledger Fabric (v2.5) et a tiré parti de l'environnement WSL2 sur une machine Windows 10, combiné à Docker Desktop, pour assurer la virtualisation des composants de la blockchain.

10.1 Préparation de l'Environnement

L'environnement de développement a été mis en place sur un système Windows 11 doté de WSL2, avec une distribution Ubuntu 20.04. Docker Desktop a été installé et configuré pour allouer 6 Go de mémoire spécifiquement aux conteneurs Hyperledger Fabric, ce qui a permis un fonctionnement fluide du réseau simulé.

Les outils en ligne de commande d'Hyperledger Fabric, tels que peer, ont été installés, et leur bon fonctionnement a été vérifié via la commande suivante :

```
    peer version && docker --version
```

L'organisation du projet a été pensée pour favoriser la clarté et la modularité. L'arborescence se présente ainsi :

```
usine-eau-fabric/
          network/
                crypto-config.yaml
                configtx.yaml
                docker-compose.yml
          chaincode/
                traceability.js
          scripts/
              deploy.sh
              test.sh
```

10.2 Mise en place de la sécurité et des identités

La sécurité étant primordiale dans un système blockchain, nous avons commencé par configurer le système d'identités cryptographiques. Le fichier crypto-config.yaml a été méticuleusement préparé pour définir notre organisation peer (entrepôt.usine-eau.local) avec un nœud principal et deux comptes utilisateurs. L'exécution de la commande cryptogen a généré l'ensemble des certificats nécessaires, organisés dans une structure de répertoires reflétant la hiérarchie organisationnelle. Nous avons validé cette étape en inspectant manuellement les certificats générés et en vérifiant leur emplacement correct dans l'arborescence des fichiers. L'étape suivante a consisté à définir les entités organisationnelles du réseau blockchain à l'aide du fichier 'crypto-config.yaml'. Deux organisations ont été spécifiées : l'organisation Orderer et une organisation Peer (nommée 'entrepôt.usine-eau.local') comprenant un nœud principal et deux utilisateurs (Admin et User1). La génération des certificats s'est effectuée avec la commande suivante :

```
cryptogen generate --config=network/crypto-config.yaml --output=
```

```
    "network/crypto-config"
```

L'intégrité de la structure générée a été validée par une inspection de l'arborescence des répertoires :

```
    tree network/crypto-config -L 3
```

Cette vérification a permis de s'assurer que les certificats étaient correctement générés pour les peers et les utilisateurs.

10.3 Création des Artefacts Réseau

La configuration du réseau a ensuite nécessité la création des artefacts fondamentaux via le fichier 'configtx.yaml'. Deux profils y ont été définis : un profil 'OrdererGenesis', reposant sur le consensus SOLO, et un second profil pour la création du canal de traçabilité.

Les artefacts nécessaires ont été générés à l'aide des commandes suivantes :

```
    configtxgen -profile UsineEauOrdererGenesis -outputBlock network/
        genesis.block

    configtxgen -profile UsineEauChannel -outputCreateChannelTx
        network/channel.tx
```

Les fichiers binaires générés (genesis.block et channel.tx) ont ensuite été vérifiés pour confirmer leur validité :

```
    file network/genesis.block network/channel.tx
```

10.4 Démarrage du Réseau

L'infrastructure réseau a été déployée à l'aide de Docker Compose. Le fichier 'docker-compose.yml' a été soigneusement configuré pour exposer les ports nécessaires (7050 pour l'orderer, 7051 pour le peer), monter les volumes contenant les certificats et définir les variables d'environnement critiques.

Le lancement des conteneurs s'est effectué par la commande suivante :

```
    docker-compose -f network/docker-compose.yml up -d
```

Le bon démarrage du réseau a été confirmé en vérifiant le statut des conteneurs :

```
    docker ps --format "table {{.Names}}\t{{.Status}}\t{{.Ports}}"
```

Deux conteneurs actifs devaient alors être visibles dans un état « Up », indiquant le bon fonctionnement des services.

10.5 Création du Canal

Le canal de communication, essentiel au fonctionnement du réseau Fabric, a été nommé traceability-channel. Avant sa création, les variables d'environnement ont été définies pour spécifier les chemins d'accès aux fichiers de configuration et aux certificats administrateurs :

```
    export FABRIC_CFG_PATH=\$PWD/network
```

```
export CORE_PEER_MSPCONFIGPATH=$PWD/network/crypto-config/
    peerOrganizations/entrepot.usine-eau.local/users/
    Admin@entrepot.usine-eau.local/msp
```

La création du canal s'est faite avec la commande suivante :

```
peer channel create -o localhost:7050 -c traceability-channel -f
    network/channel.tx --tls --cafile network/crypto-config/
    ordererOrganizations/usine-eau.local/tlsca/tlsca.usine-eau.
    local-cert.pem
```

La réussite de cette opération a été confirmée par la présence du fichier traceability-channel.block, dont la taille devait dépasser 1 Ko.

10.6 Déploiement du Chaincode

Le smart contract (ou chaincode) a été implémenté en JavaScript (traceability.js). Il a été d'abord empaqueté dans une archive '.tar.gz', puis installé, approuvé et enfin commité sur le canal.

Voici le processus détaillé :

- **Packaging :**

```
peer lifecycle chaincode package traceability.tar.gz --path
    ./chaincode --lang node --label traceability_1.0
```

- **Installation :**

```
peer lifecycle chaincode install traceability.tar.gz
```

- **Approbation :**

```
peer lifecycle chaincode approveformyorg \
  --channelID traceability-channel \
  --name traceability \
  --version 1.0 \
  --package-id traceability_1.0:3f7a9b8c5d4e3a1b2c6f8e9d0a4b5c7d
       8e9f0a1b6c7d8e9f0a1b2c3d4e5f6a7 \
  --sequence 1 \
  --tls \
  --cafile network/crypto-config/ordererOrganizations/usine-eau
       .local/tlsca/tlsca.usine-eau.local-cert.pem
```

- **Commit final :**

```
peer lifecycle chaincode commit \
    --channelID traceability-channel \
    --name traceability \
    --version 1.0 \
    --sequence 1 \
    --tls \
```

```
    --cafile network/crypto-config/ordererOrganizations/usine-eau
        .local/tlsca/tlsca.usine-eau.local-cert.pem \
    --peerAddresses localhost:7051 \
    --tlsRootCertFiles network/crypto-config/peerOrganizations/
        entrepot.usineeau.local/peers/peer0.entrepot.usine-eau.
        local/tls/ca.crt
```

10.7 Tests Fonctionnels

Des tests ont été réalisés afin de valider le bon fonctionnement de l'application. Un premier test a permis la création d'un lot d'eau avec un identifiant unique :

```
peer chaincode invoke \
    -C traceability-channel \
    -n traceability \
    -c '{"Args":["createLotEau","LOT001","UsineA","{\"pH\":7.2}"]}' \
    --tls \
    --cafile network/crypto-config/ordererOrganizations/usine-eau.
        local/tlsca/tlsca.usine-eau.local-cert.pem \
    --peerAddresses localhost:7051 \
    --tlsRootCertFiles network/crypto-config/peerOrganizations/
        entrepot.usineeau.local/peers/peer0.entrepot.usine-eau.
        local/tls/ca.crt
```

Un second test a permis de consulter l'historique du lot créé :

```
peer chaincode query \
    -C traceability-channel \
    -n traceability \
    -c '{"Args":["getHistory","LOT001"]}'
```

10.8 Résolution des problèmes rencontrés

Plusieurs défis techniques sont apparus au cours de l'implémentation, chacun ayant donné lieu à une analyse et une résolution méthodique. Les problèmes de connectivité entre WSL et Docker ont été résolus par l'utilisation de host-gateway pour la résolution DNS. Une expiration inattendue de certificats a nécessité leur régénération complète via cryptogen. Certaines erreurs de déploiement de chaincode ont été diagnostiquées par l'examen approfondi des logs Docker et résolues par la vérification des chemins d'accès aux certificats TLS. Ces difficultés et leurs solutions ont considérablement enrichi notre compréhension pratique des subtilités d'Hyperledger Fabric.

10.9 Bilan de l'implémentation

Cette implémentation complète a démontré la faisabilité technique d'une solution blockchain industrielle basée sur Hyperledger Fabric. Chaque étape, depuis la génération des identités jusqu'aux tests finaux, a été documentée et validée systématiquement. Le réseau résultant offre une base solide pour la traçabilité des lots d'eau, tout en restant extensible pour de futures améliorations. Les défis surmontés ont fourni des enseignements précieux qui guideront les phases ultérieures d'industrialisation et de déploiement à plus grande échelle.

Cette expérience pratique a également validé l'adéquation d'Hyperledger Fabric aux besoins spécifiques du secteur industriel que nous ciblons.

11 Apports concrets de la solution proposée

L'intégration de Hyperledger Fabric au sein du processus industriel offre plusieurs avantages majeurs :

Critère	**Apports de la solution**
Qualité	Vérification automatique des données et du poids ; détection rapide des anomalies ; traçabilité complète des lots.
Coût	Réduction des pertes liées aux erreurs humaines ; diminution des audits manuels ; baisse des coûts de non-conformité.
Temps	Automatisation des vérifications ; enregistrement instantané ; accès rapide à l'historique des événements.
Transparence	Visibilité globale sur les opérations pour les acteurs internes.
Fiabilité des données	Historique immuable et infalsifiable grâce à la technologie blockchain.

12 Limites et perspectives d'évolution

Malgré les nombreux bénéfices apportés par la solution, certaines limites doivent être considérées:

- La mise en œuvre initiale nécessite des ressources techniques (infrastructure, formation, accompagnement).
- Une montée en compétence est requise pour les équipes internes afin d'assurer une utilisation et une maintenance efficaces du système.
- L'interfaçage avec les systèmes existants peut engendrer des adaptations techniques spécifiques.

Cependant, les perspectives d'évolution sont prometteuses. La solution peut :

- Être étendue à d'autres lignes de production (boissons, sirops, etc.).
- S'intégrer avec des dispositifs IoT pour automatiser davantage la collecte de données (capteurs de température, de poids, etc.).
- S'interconnecter avec des systèmes partenaires externes (transporteurs, distributeurs) pour étendre la traçabilité au-delà du site de production.

13 Conclusion

Dans un environnement industriel en perpétuel mouvement, caractérisé par une numérisation progressive des processus et une demande renforcée de transparence, de traçabilité et de sûreté, la technologie blockchain se positionne comme une solution novatrice face aux enjeux

actuels. Ce mémoire est consacré à l'étude et à la mise en application d'Hyperledger Fabric, une plateforme de blockchain autorisée, dans le but de prouver son adéquation à un contexte industriel.

Nous avons initialement examiné les exigences particulières de l'industrie, y compris la sécurisation des lignes de production, la gestion des irrégularités et l'assurance de l'intégrité des données. Ces besoins ont conduit à l'examen d'une solution décentralisée, robuste et fiable. L'approche Hyperledger Fabric s'est démarquée grâce à sa compétence à instaurer des canaux privés, à gérer précisément les droits d'accès et à mettre en œuvre des smart contracts (chaincode) ajustables aux normes industrielles.

La solution suggérée a conduit à l'établissement d'un système de suivi solide, fondé sur deux voies séparées, l'une réservée à la production régulière et l'autre consacrée au traitement des irrégularités, tout en garantissant la confidentialité entre les différentes organisations et l'intégrité des opérations. Les expériences menées ont prouvé qu'il était possible d'intégrer Hyperledger Fabric dans un cadre industriel concret, favorisant une plus grande transparence, diminuant les chances de falsification des informations, et renforçant la confiance entre les participants de la chaîne de valeur.

Toutefois, il est crucial d'admettre que l'implémentation d'une telle technologie n'est pas sans défis, qu'ils soient d'ordre technique, organisationnel ou humain. Il reste à approfondir certaines questions concernant la scalabilité, l'interopérabilité avec les systèmes existants et l'acceptation du changement pour faciliter un déploiement à grande échelle. En somme, cette œuvre débloque la voie pour de nouvelles perspectives de recherche et d'implémentations concrètes. Il prouve que l'incorporation de la blockchain, notamment d'Hyperledger Fabric, dans le secteur industriel n'est plus un rêve irréalisable, mais une progression naturelle et encourageante vers des systèmes de production plus intelligents, plus sécurisés et interconnectés.

Conclusion générale

Le passage à l'industrie 4.0 transforme radicalement les modèles de production, de contrôle et d'administration des systèmes industriels. Cette transformation, même si elle est pionnière, entraîne une vulnérabilité accrue à des menaces de cybersécurité, surtout à cause de la fusion entre les technologies de l'information (IT) et les technologies opérationnelles (OT). Dans un contexte d'interconnexion croissante, il est crucial de sécuriser les systèmes de contrôle industriel (ICS), non seulement pour maintenir la continuité des opérations, mais aussi pour protéger les infrastructures essentielles et les informations sensibles. Dans le cadre de ce mémoire, nous avons exposé les failles inhérentes aux systèmes de contrôle industriels traditionnels, tout en mettant en évidence les contraintes des méthodes de sécurité conventionnelles. Devant ces observations, nous avons étudié les possibilités offertes par la technologie blockchain, en particulier Hyperledger Fabric, comme outil d'innovation pour améliorer la robustesse, le suivi et la fiabilité des systèmes industriels. Tout d'abord, nous avons effectué une vue d'ensemble des systèmes de contrôle industriel, en étudiant leur structure, leur mode de fonctionnement et les enjeux de sécurité qui en résultent. Cette première phase nous a aidés à saisir les particularités du secteur industriel, qui est fréquemment marqué par des exigences rigoureuses en matière de disponibilité, de fiabilité et d'opération en temps réel. Par la suite, nous avons effectué un état de l'art détaillé sur Hyperledger Fabric, une plateforme blockchain privée élaborée pour servir les exigences des consortiums industriels. Avec des attributs comme la modularité, les canaux privés, les smart contracts et le contrôle d'accès granulaire, ce système s'avère être une option appropriée pour répondre aux besoins des contextes sensibles où la confidentialité, la gouvernance et l'efficacité sont des éléments essentiels. Pour finir, nous avons suggéré une approche pratique d'architecture distribuée pour une usine de production d'eau minérale. Cette approche est structurée autour de deux flux : un flux consacré à la chaîne de production standard et un autre réservé au traitement des anomalies. Ce modèle s'inspire de l'organisation observée au sein de la SARL IBRAHIM et Fils IFRI, une entreprise locale dont les processus de production ont constitué une base de réflexion concrète pour la conception de notre proposition. Grâce à cette structure, nous avons montré comment assurer un suivi des opérations, la protection des données et une meilleure résistance aux erreurs ou aux cyberattaques, tout en assurant la clarté entre les divers participants du processus. Ainsi, notre démarche ne se limite pas à la sécurisation des données, elle propose également un modèle de gouvernance décentralisée qui favorise une supervision industrielle fiable, transparente et collaborative. Cette perspective pave la voie vers des horizons inédits pour le secteur industriel, où la confiance n'est plus supposée, mais démontrée, enracinée dans un registre décentralisé et indestructible. Pour résumer, cette étude souligne l'importance d'intégrer la blockchain dans les secteurs industriels, non pas en tant que technologie substitutive, mais comme un appui supplémentaire pour consolider les infrastructures actuelles. Elle propose également une perspective innovante sur la sécurité basée sur la décentralisation, l'auditabilité et la résilience. Les recherches futures pourraient inclure l'extension de cette solution à d'autres domaines industriels, l'incorporation

de systèmes d'intelligence artificielle pour la prédiction des anomalies, ou encore l'évaluation des performances et de la capacité à l'échelle de l'architecture proposée dans des contextes réels et d'envergure. Ces perspectives mettent en évidence à la fois l'abondance et le potentiel révolutionnaire de la blockchain dans l'industrie contemporaine.

Bibliographie

[1] Monzer, M. H. (2020). *Model-based IDS design pour ICS* (Doctoral dissertation, Université Grenoble Alpes [2020-....]; Université Libanaise).

[2] Kondah, H. (s.d.). *La cybersécurité des systèmes industriels* [Vidéo YouTube]. Récupéré de https://www.youtube.com/watch?v=qt7qJ1Faf7o

[3] Agence nationale de la sécurité des systèmes d'information. (2012, juin). *La cybersécurité des systèmes industriels* (Version 1.0) [Guide]. France.

[4] Keith, S., et al. (2015, mai). *Guide to Industrial Control Systems (ICS) Security* (NIST Special Publication 800-82, Revision 2). États-Unis.

[5] Lee, S. L., et al. (2015, mars). Modernizing pharmaceutical manufacturing: From batch to continuous production. *Journal of Pharmaceutical Innovation.*

[6] Infor. (2024, novembre 7). *Que sont les industries de distribution ?* [Site internet]. Récupéré de https://www.infor.com/fr-fr/distribution-industries

[7] Badot, O., Lemoine, J.-F., Ochs, A. (2021). Distribution 4.0 (2 éd.). Pearson.

[8] Industrie Distribution. (2024, août 7). *Conseils en ingénierie et performance industrielle* [Site internet]. Récupéré de https://www.industrie-distribution.com/

[9] Ikene, I., Boucif, M. (2023). *Cybersécurité ICS-SCADA* [Mémoire de master en informatique]. Université de Béjaïa, Algérie.

[10] Tulip. (2024, avril 10). *IT vs OT : Difference between Information Technology and Operational Technology.* Récupéré de https://tulip.co/fr/blog/it-vs-ot-difference-between-information-technology-and-operational-technology/

[11] Macaulay, T., Singer, B. L. (2011). Cybersecurity for industrial control systems: SCADA, DCS, PLC, HMI, and SIS. CRC Press.

[12] kaspersky Labs.(2024).*Threat landscape for industrial automation systems Q2 2024* Récupéré de https://ics-cert.kaspersky.com/publications/reports/2024/11/21/threat-landscape-for-industrial-automation-systems-regions-q2-2024/

[13] Fortinet. (2024, juin). State of Operational Technology and Cybersecurity Report. FortinetFortiGuardLabs. Retrieved from Fortinet website

[14] Cisco. (2024). *Qu'est-ce que la sécurité OT ?* Récupéré de https://www.cisco.com/site/fr/fr/learn/topics/security/what-is-ot-security.html

[15] Seminar IITM WS 21/22, Network Architectures and Services. (Mai 2022). Review of Industrial Control Systems Protocols.

[16] Micode. (2024, 27 décembre). La première cyberarme de l'Histoire [Vidéo]. YouTube. https://www.youtube.com/watch?v=gXtp6C-3JKo

[17] Yli-Huumo, J., Ko, D., Choi, S., Park, S., Smolander, K. (2016). Where is current research on blockchain technology?—A systematic review. PLOS ONE, 11(10), e0163477. https://doi.org/10.1371/journal.pone.0163477

[18] Tian, F. (2017). A supply chain traceability system for food safety based on HACCP, blockchain Internet of things. 2017 International Conference on Service Systems and Service Management, 1–6. https://doi.org/10.1109/ICSSSM.2017.7996119

[19] Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, et al. (2018). Hyperledger Fabric: A distributed operating system for permissioned blockchains. Proceedings of the Thirteenth EuroSys Conference, 1–15. https://doi.org/10.1145/3190508.3190538

[20] Baliga, A. (2017). Understanding Blockchain Consensus Models. Persistent Systems Technical Report. https://pdfs.semanticscholar.org

[21] Saberi, S., Kouhizadeh, M., Sarkis, J., Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. International Journal of Production Research, 57(7), 2117–2135. https://doi.org/10.1080/00207543.2018.1533261

[22] Thakkar, P., Nathan, S., Viswanathan, B. (2018). Performance benchmarking and optimizing Hyperledger Fabric blockchain platform. 2018 IEEE 26th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS), 264–276. https://doi.org/10.1109/MASCOTS.2018.00041

[23] Ahmad, R. W., Hasan, H. R., Jayaraman, R., Salah, K. et al (2022). Integrating Lean Six Sigma with blockchain technology for quality management: A conceptual framework and research agenda. *Renewable and Sustainable Energy Reviews*, 131, 110030. https://doi.org/10.1016/j.rser.2020.110030

[24] Sicard, N. (2023). Méthodologie de conception et d'implémentation de la technologie blockchain dans le secteur industriel [Mémoire de maîtrise, Université du Québec à Trois-Rivières]. Université du Québec à Trois-Rivières.

[25] Sinha, S., Chui, C.-K. (2021). Blockchain in manufacturing quality control: A computer vision-based framework. PLOS ONE, 16(3), e0247925. https://doi.org/10.1371/journal.pone.0247925

[26] Zhang, Y., Wen, J. (2017). The IoT electric business model: Using blockchain technology for the internet of things. Peer-to-Peer Networking and Applications, 10(4), 983–994. https://doi.org/10.1007/s12083-016-0456-1

[27] Wang, C., Chu, X. (2020). Performance characterization and bottleneck analysis of Hyperledger Fabric. arXiv preprint arXiv:2008.05946. https://arxiv.org/abs/2008.05946

[28] Liu, Y., Wang, X. (2023). A comprehensive Hyperledger Fabric performance evaluation based on stochastic Petri nets. Cluster Computing, 26(3), 1235–1248. https://doi.org/10.1007/s10586-023-03567-9

[29] Kumar, R., Tripathi, R. (2024). Performance benchmarking of Hyperledger Fabric networks: Insights for enterprise deployment. Lecture Notes in Computer Science, 13999, 1–15. https://doi.org/10.1007/978-981-97-3698-0_1

[30] Francisco, K., Swanson, D. (2018). The supply chain has no clothes: Technology adoption of blockchain for supply chain transparency. Logistics, 2(1), 2. https://doi.org/10.3390/logistics2010002

[31] IBM. (2018). IBM Food Trust: Blockchain for the world's food supply. IBM Corporation. Retrieved from https://www.ibm.com/blockchain/solutions/food-trust

[32] Carrefour. (2019). Carrefour blockchain food traceability project. Retrieved from https://www.carrefour.com/en/newsroom/carrefour-blockchain

[33] Salah, K., Rehman, M. H. U., Nizamuddin, N., Al-Fuqaha, A. (2019). Blockchain for AI: Review and open research challenges. IEEE Access, 7, 10127–10149. https://doi.org/10.1109/ACCESS.2019.2890507

[34] Kamath, R. (2018). Food traceability on blockchain : Walmart's pork and mango pilots with ibm. The Journal of the British Blockchain Association, 1:1–12. doi : 10.31585/jbba-1-1-(10)2018

[35] Ahmad, R. W., Al Khader, W., Jayaraman, R., Salah, K., Antony, J., Swarnakar, V. (2022). Integrating Lean Six Sigma with blockchain technology for quality management – a scoping review of current trends and future prospects. The TQM Journal, 35(7), 1609–1631. https://doi.org/10.1108/TQM-06-2022-0181

[36] Rathi, R., Singh, M., Antony, J., Garza-Reyes, J. A., Goyat, R., Shokri, A. (2024). Integration of blockchain and Lean Six Sigma approach for operational excellence: a proposed model. International Journal of Lean Six Sigma. https://doi.org/10.1108/IJLSS-07-2022-0148

[37] Cachin, C. (2016). Architecture of the Hyperledger blockchain fabric. Workshop on Distributed Cryptocurrencies and Consensus Ledgers (Vol. 310, pp. 1–4). https://doi.org/10.3929/ethz-a-010620078

[38] Sousa, J., Bessani, A., Vukolić, M. (2018). A Byzantine fault-tolerant ordering service for the Hyperledger Fabric blockchain platform. In 2018 IEEE 48th Annual International Conference on Dependable Systems and Networks (DSN) (pp. 51–58). IEEE. https://doi.org/10.1109/DSN.2018.00018

[39] Mougayar, W. (2016). The Business Blockchain: Promise, Practice, and the Application of the Next Internet Technology. Wiley.

[40] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

[41] Gorenflo, C., Lee, S., Golab, L., Keshav, S. (2020). FastFabric: Scaling Hyperledger Fabric to 20,000 Transactions per Second. Proceedings of the 2020 ACM SIGMOD International Conference on Management of Data, 1–15. https://doi.org/10.1145/3318464.3382563

[42] IBM. (2023). Explore Hyperledger Fabric Ledger using the Node.js SDK. IBM Developer Documentation. https://developer.ibm.com/articles/explore-hyperledger-fabric-ledger/

[43] Baudet, M., Chatterjee, R., David, B., Gazi, et al (2020). SoK: Communication Across Distributed Ledgers. IEEE European Symposium on Security and Privacy Workshops (EuroSPW), 138–151. https://doi.org/10.1109/EuroSPW51379.2020.00025

[44] Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. Applied Innovation, 2, 6–10.

[45] Sharma, M., Gupta, S. (2020). Hands-On Smart Contract Development with Hyperledger Fabric V2: Building Enterprise Blockchain Applications. Packt Publishing.

[46] Hyperledger Fabric. Blockchain. consulté le 8 avril 2025, https://hyperledger-fabric.readthedocs.io/en/release-2.5/blockchain.html

[47] Vacca, J. R. (2020). Blockchain and the Hyperledger Fabric: Enterprise-grade blockchain for the business world. Syngress.

[48] Lantz, L., Cawrey, D. (2021). Mastering Blockchain: Unlocking the power of cryptocurrencies, smart contracts, and decentralized applications. O'Reilly Media.

[49] Journal du Coin. DLT (Distributed Ledger Technology). Journal du Coin. Consulté le 14 février 2025, à l'adresse https://journalducoin.com/lexique/dlt/

[50] Zand, M., Wu, X., Morris, M. A. (2021). Hands-On Smart Contract Development with Hyperledger Fabric V2. O'Reilly Media.

[51] Bazizi, S., Beldjoudi, C. (2020). Conception et réalisation d'une blockchain : Cas d'étude – gestion du dossier de santé électronique (Mémoire de master). Université de Bejaia.

[52] CDBF. (n.d.). Blockchain privée. Consulté le 14 février 2025, à l'adresse https://cdbf.ch/lexique/blockchain-privee/

[53] Adada, L., Hamidache, N. (2020). Déanonymisation de clients dans le réseau Bitcoin à l'aide de l'apprentissage automatique (Mémoire de master). Université Mouloud Mammeri de Tizi-Ouzou.

[54] Ghriba, M. (2022). L'intérêt de l'adoption de la blockchain par les entreprises : Revue systématique de la littérature (Mémoire de master). Université Paris 1 Panthéon-Sorbonne.

[55] Foley Lardner LLP. (2021, août). Types of blockchain: Public, private, and everything in between. Consulté le 14 février 2025, à l'adresse https://www.foley.com/insights/publications/2021/08/types-of-blockchain-public-private-between/

[56] Hyperledger Foundation. Blockchain overview. Consulté le 14 février 2025, à l'adresse https://hyperledger-fabric.readthedocs.io/en/release-2.5/blockchain.html

[57] Al-Jaroodi, J., Mohamed, N. (2019). Blockchain in industries: A survey. IEEE Access. https://doi.org/10.1109/ACCESS.2019.2903554

[58] Benmoussa, R., Boudjemaa, A. (2023). La blockchain pour la transition énergétique : Applications pour les réseaux électriques intelligents [Article]. HAL. https://hal.science/hal-04058669v1/document

[59] SAP. (n.d.). Qu'est-ce que l'Internet des objets (IoT)? SAP France. https://www.sap.com/france/products/technology-platform/what-is-iot.html

[60] Hyperledger. (n.d.). Hyperledger Fabric Documentation. Hyperledger Foundation. https://hyperledger-fabric.readthedocs.io/

Résumé

L'apparition de l'Industrie 4.0 révolutionne les systèmes industriels par l'intégration de l'automatisation, de la connectivité et de l'analyse intelligente des données. Cependant, ce passage expose les Systèmes de Contrôle Industriel (ICS) à des menaces de cybersécurité inédites, exacerbées par la fusion entre les technologies d'information (IT) et les technologies opérationnelles (OT). Ce travail examine la possibilité d'utiliser la blockchain, en particulier Hyperledger Fabric, pour renforcer la sécurité, la traçabilité et la robustesse des processus industriels. Suite à l'exposé des principes de base des systèmes de contrôle industriels (ICS) et des défis liés à leur sécurité, une étude détaillée sur Hyperledger Fabric est effectuée. Par la suite, une architecture de sécurité décentralisée est suggérée, basée sur un cas concret observé dans l'entreprise de production d'eau minérale SARL IBRAHIM et Fils - IFRI. La solution comprend des canaux privés pour la distinction entre les flux de production et les anomalies, ainsi qu'un contrat intelligent garantissant l'intégrité des enregistrements. Cette étude démontre que la blockchain peut avoir un impact significatif sur la sécurisation des environnements industriels critiques, tout en paveant la voie vers des modèles de gouvernance plus transparents et collaboratifs.

Mots clé : Industrie 4.0, Systèmes de Contrôle Industriel, cybersécurité industrielle, blockchain, Hyperledger Fabric.

Abstract

The rise of Industry 4.0 is reshaping industrial systems through automation, interconnectivity, and smart data processing. However, this shift also exposes Industrial Control Systems (ICS) to growing cybersecurity threats, especially due to the increasing convergence between Information Technology (IT) and Operational Technology (OT). This thesis explores the potential of blockchain technology, specifically Hyperledger Fabric, as a solution to enhance the security, traceability, and resilience of industrial processes. After presenting the foundations of ICS and the related security challenges, the work provides a detailed state-of-the-art on Hyperledger Fabric. It then proposes a decentralized security architecture inspired by real-world observations at SARL IBRAHIM et Fils – IFRI, a mineral water production company. The proposed solution includes private channels to separate production and anomaly management flows, along with a smart contract to ensure data integrity and traceability throughout the process. This study demonstrates how blockchain can serve as a powerful tool to secure critical industrial environments while promoting more transparent and collaborative governance models.

Keywords : Industry 4.0, Industrial Control Systems (ICS), cybersecurity, blockchain, Hyperledger Fabric.