



Blockchain pour le Nucléaire

focus sur le projet I3P CyberQL (Cybersécurité et Qualité Logiciel)

Önder GÜRCAN, Ingénieur Chercheur, Expert

6 Octobre 2020

Contexte, enjeux et objectifs d'EDF

Contexte et Enjeux



1

Mieux maîtriser les procédés de fabrication des équipements nucléaires

- ✓ Amélioration continue des procédés
- ✓ Améliorer la **confiance** de l'Autorité Sûreté Nucléaire (ASN)
- ✓ Dynamiser la filière



2

Acquérir et certifier les données de certains procédés clés en blockchain

- ✓ Démontrer coûts et valeurs de la **blockchain**



3

S'appuyer sur les nouvelles technologies du numérique pour améliorer la confiance et créer de la valeur

- ✓ Juguler l'extension de l'exigence de **certification** des laboratoires
- ✓ Créer de la **valeur** (nouveaux services à valeur ajoutée)

Objectif : Proposer une solution répondant aux exigences de l'arrêté Equipement Sous-Pression Nucléaire (ESPN) :

- Qui **réduit les possibilités d'erreurs** intentionnelles et/ou non-intentionnelles,
- Qui est **suffisamment standard pour être déployé** auprès de nombreux laboratoires lors du déploiement.

Contexte, enjeux et objectifs du LICIA

► En théorie:

- Une blockchain permet d'enregistrer des **données immuables**.
- Les smart-contrats permettent **d'exécuter des traitements non-répudiables**, pour contrôler la donnée enregistrée.
- Les blockchains de consortium (ou permissionnées) implémentent des mécanismes de contrôle d'accès assurant la **confidentialité des données**.

► En pratique:

- Comme pour tout **système critique**, il convient de **maîtriser la sûreté de fonctionnement** des applications blockchain.

Objectif: Développer une méthodologie de qualification d'une application Blockchain.

Surete de fonctionnement: Vivacité des transactions

- ▶ On dit qu'un système transactionnel est **vivant** si chaque transaction valide qui lui est soumise sera **exécutée à terme**.
 - Elle est **a priori assurée** dans les BC publiques grâce aux **mécanismes d'incitation**.
 - Dans Ethereum, une transaction **peut rester longtemps** en attente si l'émetteur ne **récompense pas suffisamment** les mineurs.
- ▶ **Le Risque:** La **censure** est une action malicieuse visant à contrecarrer la propriété de vivacité pour certaines transactions ciblées
 - Dans **Hyperledger Fabric**, un **approbateur** peut censurer une transaction

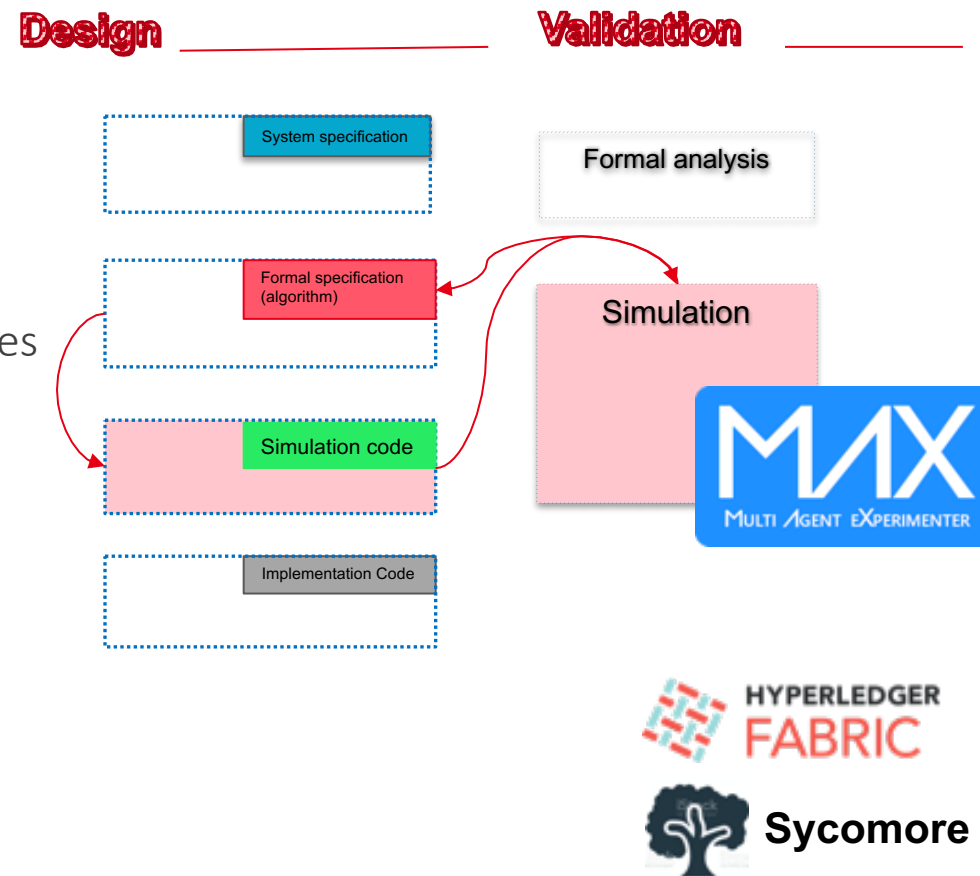
Gagner la confiance dans les protocoles Blockchain: de la spécification à la simulation

Il n'est pas toujours viable d'effectuer une analyse formelle **en raison de la complexité** du modèle du système.

- des agents intelligents,
- des attaques sophistiquées
- etc.

Le recours à la simulation est fondamental, mais **manque d'outils de simulation** pour les blockchains

- soit protocole ad-hoc
- ou trop générique

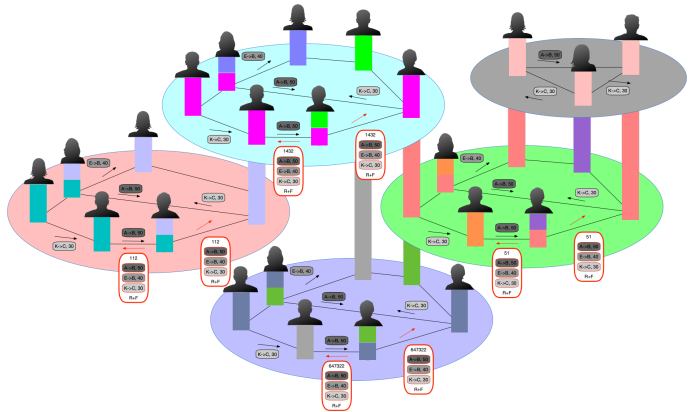
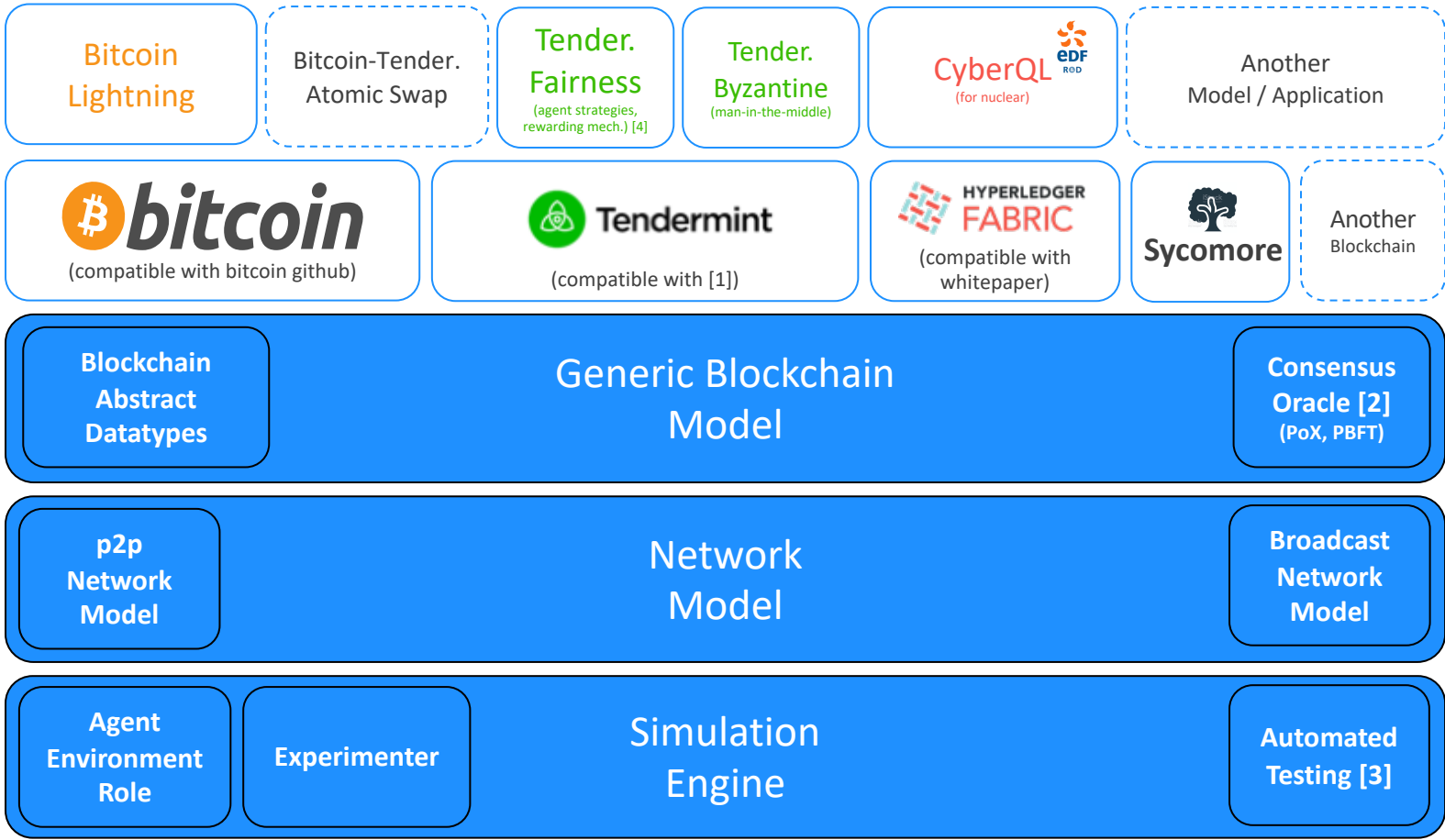


LICIA développe un simulateur pour exécuter des expériences sur des **protocoles distribués sécurisés** appelé **MAX**.

Nous analysons actuellement **Hyperledger** pour **EDF R&D** et **Sycomore** (thèse de doctorat).

- plusieurs vulnérabilités identifiées,
- scénario à risque identifié,
- et atténuation trouvée.

Multi-Agent eXperimenter (MAX)



[1] Y. Amoussou-Guenou, A. Del Pozzo, M. Potop-Butucaru, and S. Tucci-Piergiovanni, **Dissecting Tendermint**, Int. Conference on Networked Systems (NETYS 2019), pp 166-182, 2019.

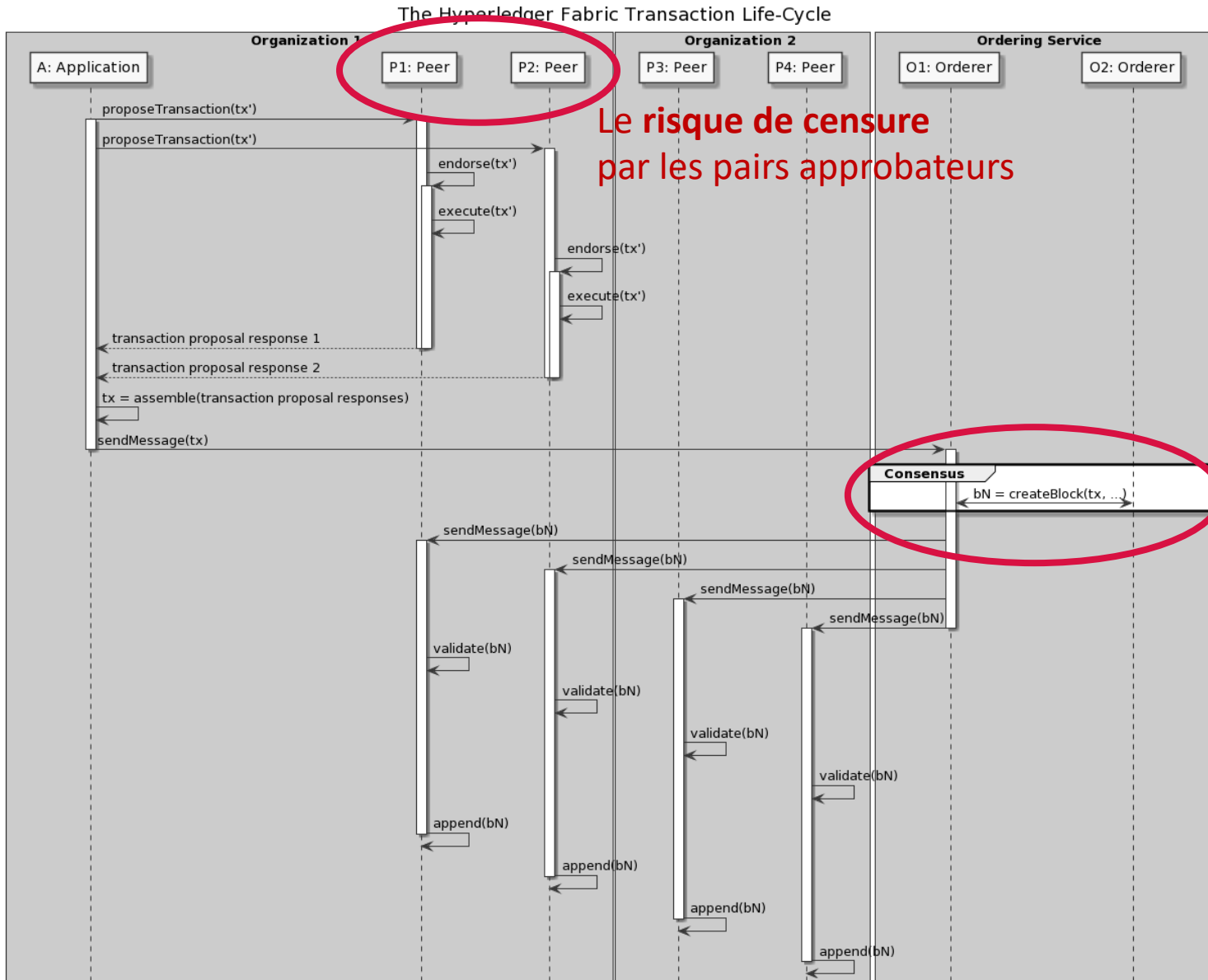
[2] E. Anceaume, A. Del Pozzo, R. Ludinard, M. Potop-Butucaru, and S. Tucci-Piergiovanni, **Blockchain Abstract Data Type**, in SPAA 2019, Phoenix, USA, June 22-24, 2019, pp. 349–358.

[3] Ö. Gürçan, O. Dikenelli, C. Bernon (2013). **A generic testing framework for agent-based simulation models**. Journal of Simulation.

[4] N. Lagaillarde, M. A. Djari, Ö. Gürçan (2019). **A Computational Study on Fairness of the Tendermint Blockchain Protocol**. Information.

Hyperledger Fabric – Cycle de Vie d'une Transaction

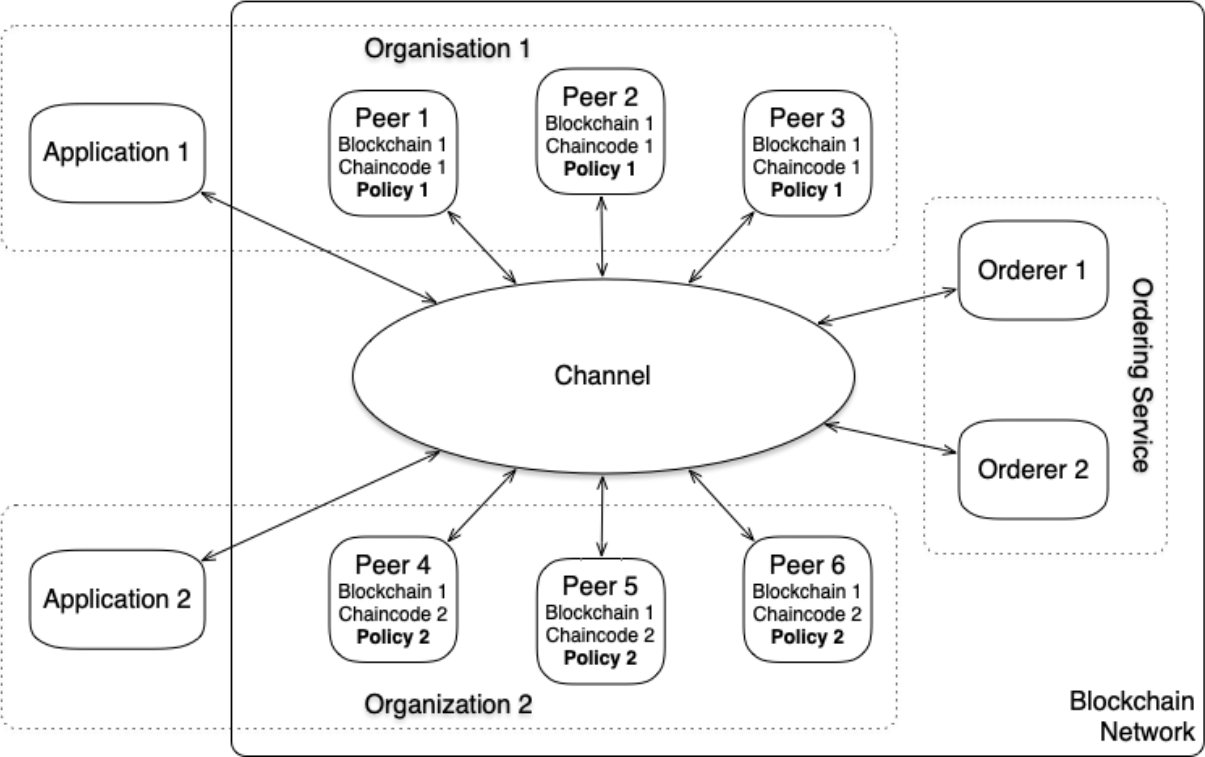
- tx est proposé
- tx est endorsé
- tx est ordonné
- tx est écrit dans BC



Le risque de censure
par les pairs approbateurs

La concurrence de
transaction conflictuels

Etude I: Le risque de censure par les pairs approbateurs

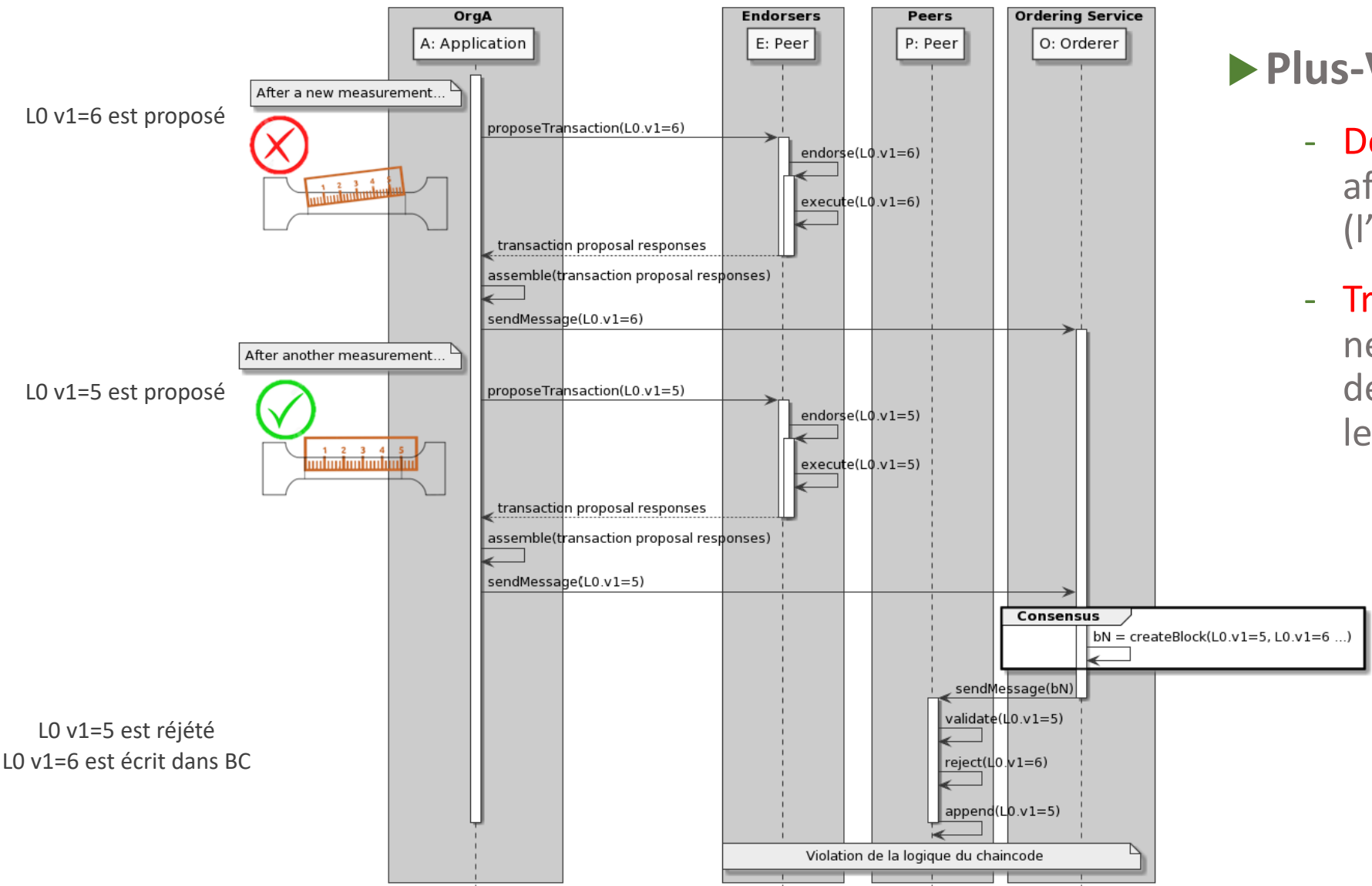


► Plus-Value apportée par le LICIA

- Trouver l'effet de différentes politiques d'approbations sur la validation d'une transaction.
- Illustration d'un cas où la politique d'approbation permet de réussir une tentative de censure,
- Illustration d'un autre où la politique d'approbation la fait échouer.
- Sélectionner les bon politiques d'approbation.

Etude 2: La concurrence des transactions conflictuelles

Le problème de la gestion des transactions parallèles conflictuelles (le scénario à étudier)



► Plus-Value apportée par le LICIA

- **Détection le cas conflictuel** et affichage à l'utilisateur final (l'auditeur).
- **Trouver le temps minimum** nécessaire pour effectuer le deuxième transaction pour **éviter** le conflit.

L0.v1=5 est réjeté
L0.v1=6 est écrit dans BC

Réalisation du modèle et des scenarios

The screenshot displays the Eclipse IDE interface with the following components:

- Package Explorer:** Shows the project structure. The path `max.model.ledger.hyperledgerfabric > src/main/java > max.model.ledger.hyperledgerfabric` is selected, highlighting `HFAApplication.java`.
- Editor:** Displays the code for `HFAApplication`. The class is annotated with `HFApplication<Tx extends Transaction>`. The code includes:
 - A `schedule` method call at the top.
 - An `@Override` method `proposeTransaction` that creates a PROPOSE message, gets the agent address, creates a propose message, and sends it via the network environment.
 - An `@Override` method `handleMessage` that switches on the message type, handling `PROPOSAL_RESPONSE` messages.
 - A private method `handleProposalResponseMessage` for checking responses.
- Outline:** Shows the class `HFAApplication<Tx extends Transaction>` with its methods: `makeInitialPlan()`, `proposeTransaction`, `handleMessage`, and `handleProposalResponseMessage`.
- Task List:** Empty.
- Bottom Bar:** Includes tabs for Problems, Javadoc, Declaration, Git Repositories, Search, Console, Progress, Git Staging, Call Hierarchy, and Synchronize.

Travaux en cours et futurs

► Travaux en cours

- Implementation du modèle Hyperledger Fabric et les scenarios conçu en MAX.
- Analyse des resultats obtenus.

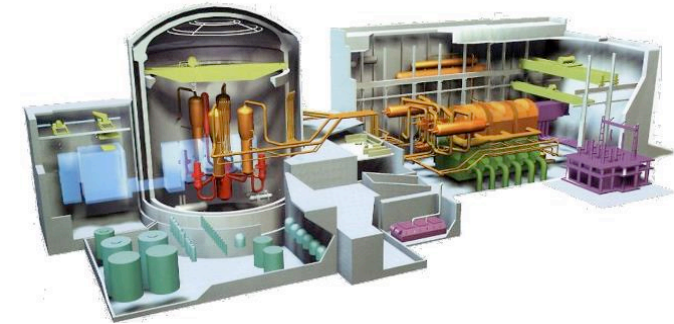
► Travaux futurs

- Amelioration du modèle Hyperledger Fabric (dont les smart contrats).
- Conception des nouveaux scenarios.

On a focalisé sur CyberQL mais en parallele ...

► On travaille sur le projet Réacteur Numérique (EDF)

- Un **jumeau numérique du réacteur nucléaire** couvrant les phases de conception, d'exploitation et de déconstruction sous la forme d'une plateforme commune pour :
 - améliorer la performance de la filière nucléaire via un simulateur d'entraînement pour les exploitants,
 - bâtir de nouvelles offres numériques à l'export via des services de simulation.



► Plus-Value apportée par le LICIA

- La **sécurisation** des données et des codes de la plateforme,
- La **transparence** de la facturation.



Merci pour votre attention!

Önder GÜRCAN