ENGISIS

INTEROPERABILITY FOR PRODUCT LIFECYCLE MANAGEMENT

Application of blockchain and standards-based interoperability to manufacturing and MRO in a MBE

Xenia Fiorentini, CEO

Engisis

Position

Engisis provides services and technology
for PLM interoperability

Key points

- Focus on international **standards** and **model based approach**
- **International network** of industrial partners, universities and standardization committees
- **Location**: Italy, France, USA

Mission

To help our curstomers understand, design and implement a PLM strategy by:

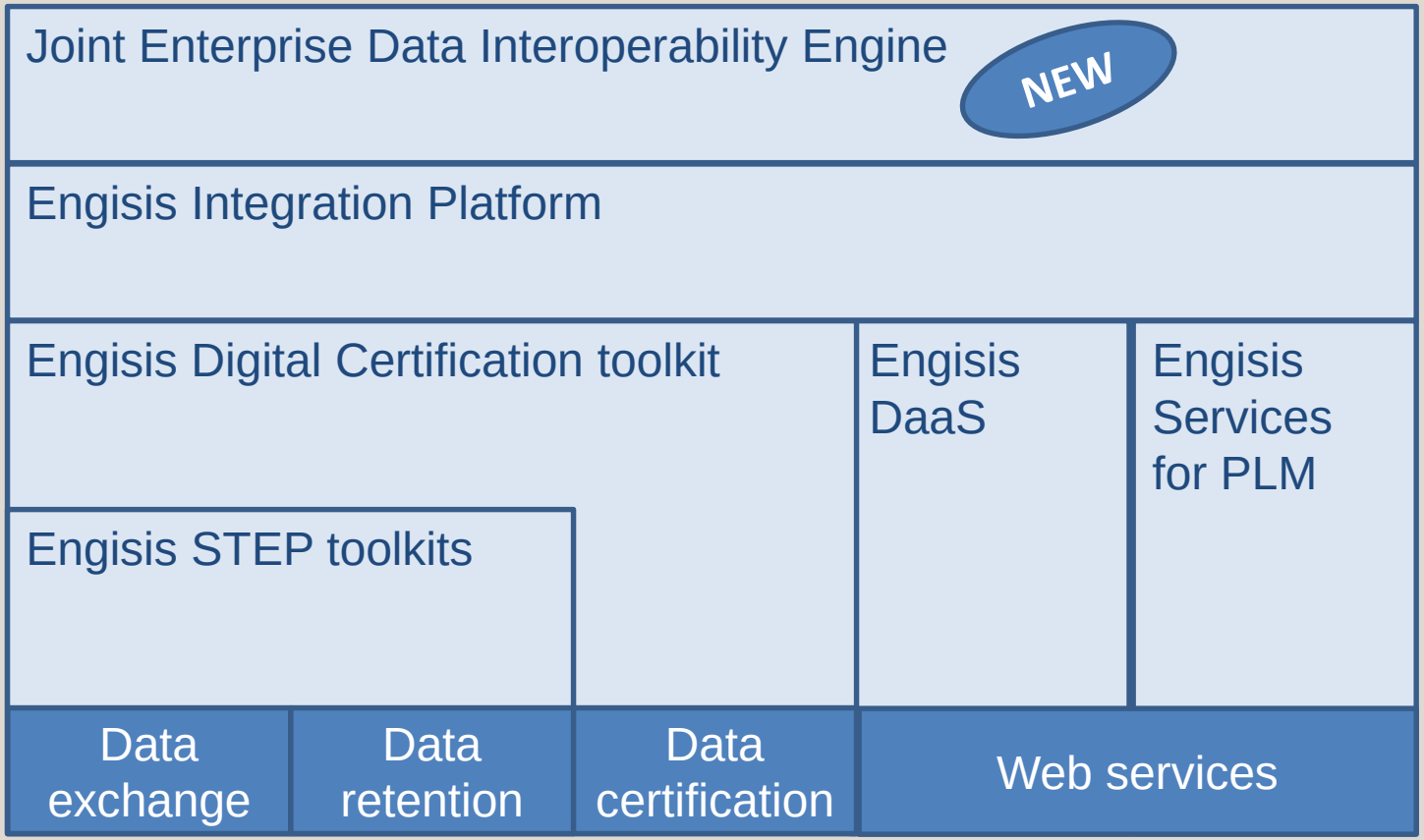
- understanding the **processes** across the lifecycle,
- designing **methods** to support these processes,
- providing the **technology** to implement data exchange and integration through the product lifecycle

Customers

Big organizations with **complex products** and **long lifecycle**

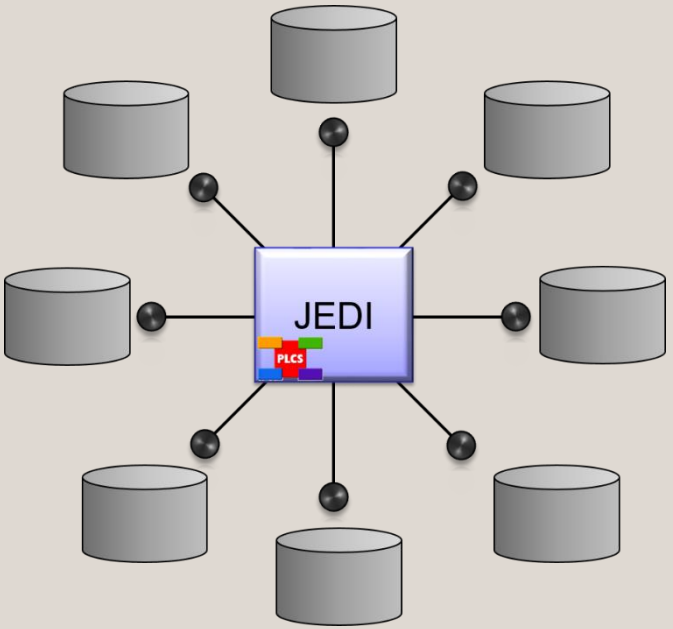
ENGISIS

The technology



Join Enterprise Data Interoperability (JEDI)

- JEDI is a capability developed through our Nexus subsidiary
- A data interoperability capability between Services and partners:
  - Interoperable equipment transactional and life-cycle data across organizations and information systems
  - Uses open standards to exchange detailed equipment data using NATO compliant ISO 10303:239 “PLCS” open data standards
  - Maximize discovery, access, and re-use of equipment data in logistics processes
  - Application within many scenarios



Current JEDI Landscape

JEDI-MAC (Marine-Army Calibration)

- US Army calibration support for USMC in production environment

JEDI-M (Maintenance)

- Demonstration in NATO CWIX exercise with US Army, USMC, and NATO partners, deployed across DoD MPE and NATO FMN

JEDI-IDSE (Integrated Digital Sustainment Environment)

- Link supply chain need for part with digital manufacturing processes

JEDI-JOPES (Joint Operations Planning & Execution System)

- Sharing of US deployment and sustainment data with NATO to coordinate operations and exercises

JEDI-M1 Abrams

- Joint/Coalition M1 tank parts inventory data integration supporting maintenance actions and fleet analyses

Challenges

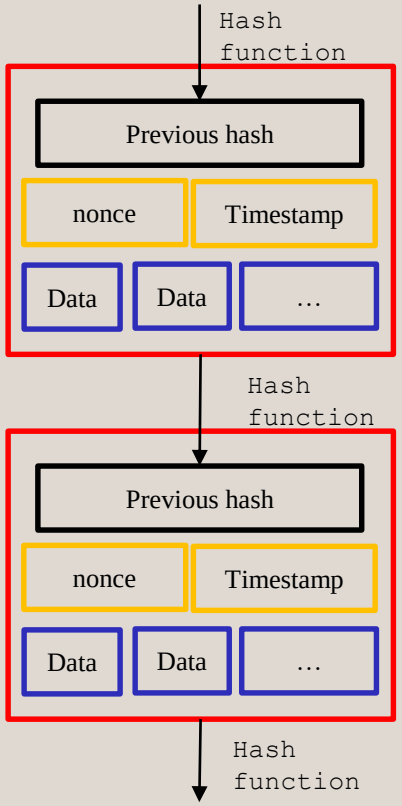
- Trust
- Data ownership
- Traceability
- Data integrity
- Fraud prevention

What is blockchain?

- Heavily used for financial transactions
  - Initially created to support the Bitcoin currency (millions USD exchanged every day)
- Decentralized ledger (of facts) on a peer-to-peer network
  - Facts are validated without the need for a central authority
  - Each fact must be validated by a majority of the peers (consensus mechanism)
    - › Validation algorithm implements the business logic
    - › Consensus implements the security
    - › The more participants, the more secure the ledger is
- A record of facts is replicated through a peer-to-peer network
- A set of facts is stored in a block (storage unit)

What is a block in the chain?

- Each block contains different information:
  - A list of facts
  - Metadata
  - A link to the previous block



Data integrity support

- Retroactive alterations impossible due to 3 principles
  1. The link between the blocks
     - › Alterations requires to partially rebuild the chain to insert new fraudulent and valid data
  2. The replication of the data
     - › Alterations would require to alter ALL replicates
  3. The consensus mechanism
     - › To alter all replicates requires control over the majority of the peers to make fraudulent data “official”

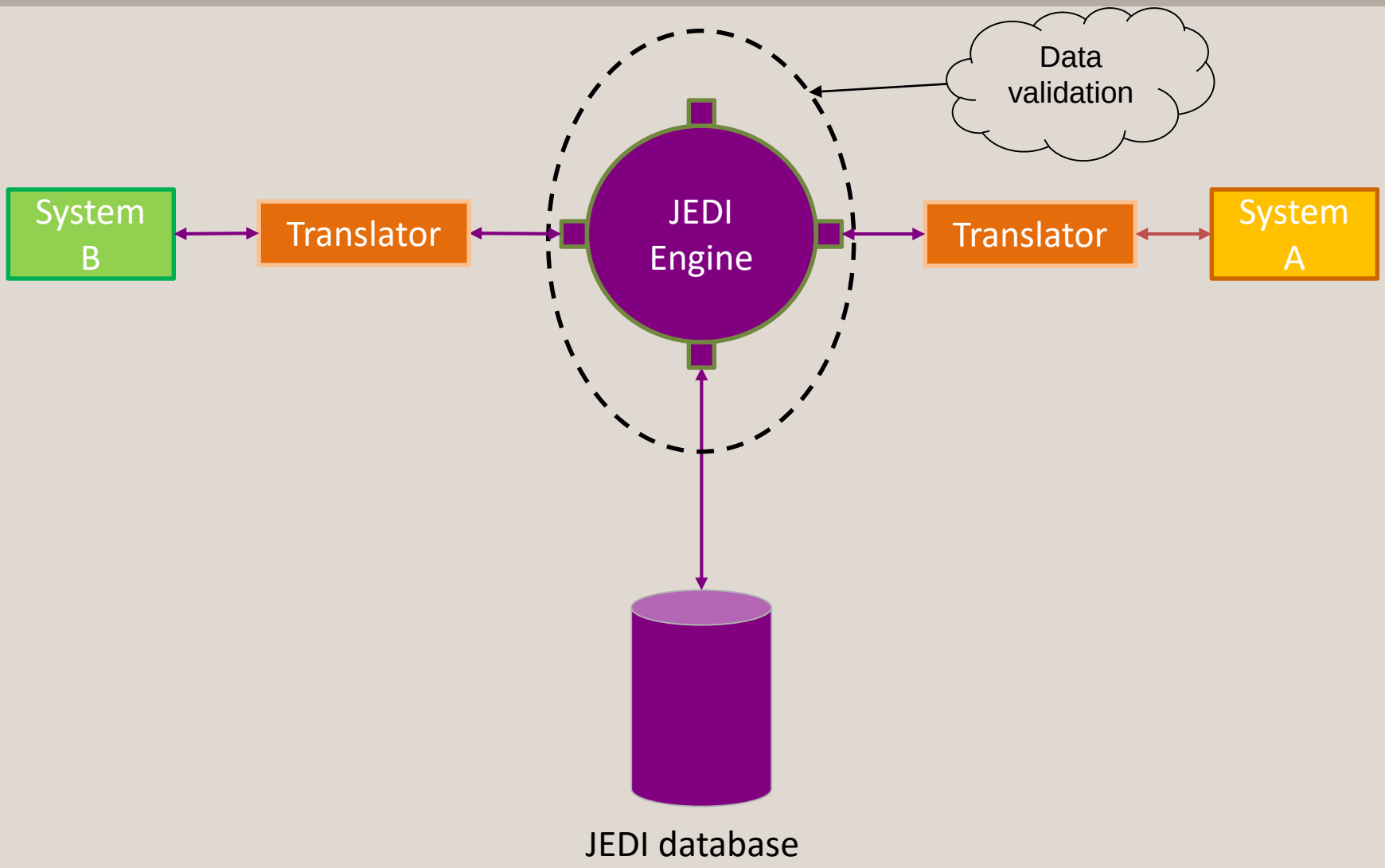
Why JEDI and blockchain?

- Blockchain is ideal within 3 conditions:
  - Large network of participants
  - Management of transactions (physical and/or virtual assets)
  - Data trust and traceability are critical
- JEDI is a strong candidate
  - Several organizations and several networks
  - Data exchange is a transaction
  - Record parts movements/exchanges between forces/allies
  - Transactions data is trustworthy enough for seamless audit

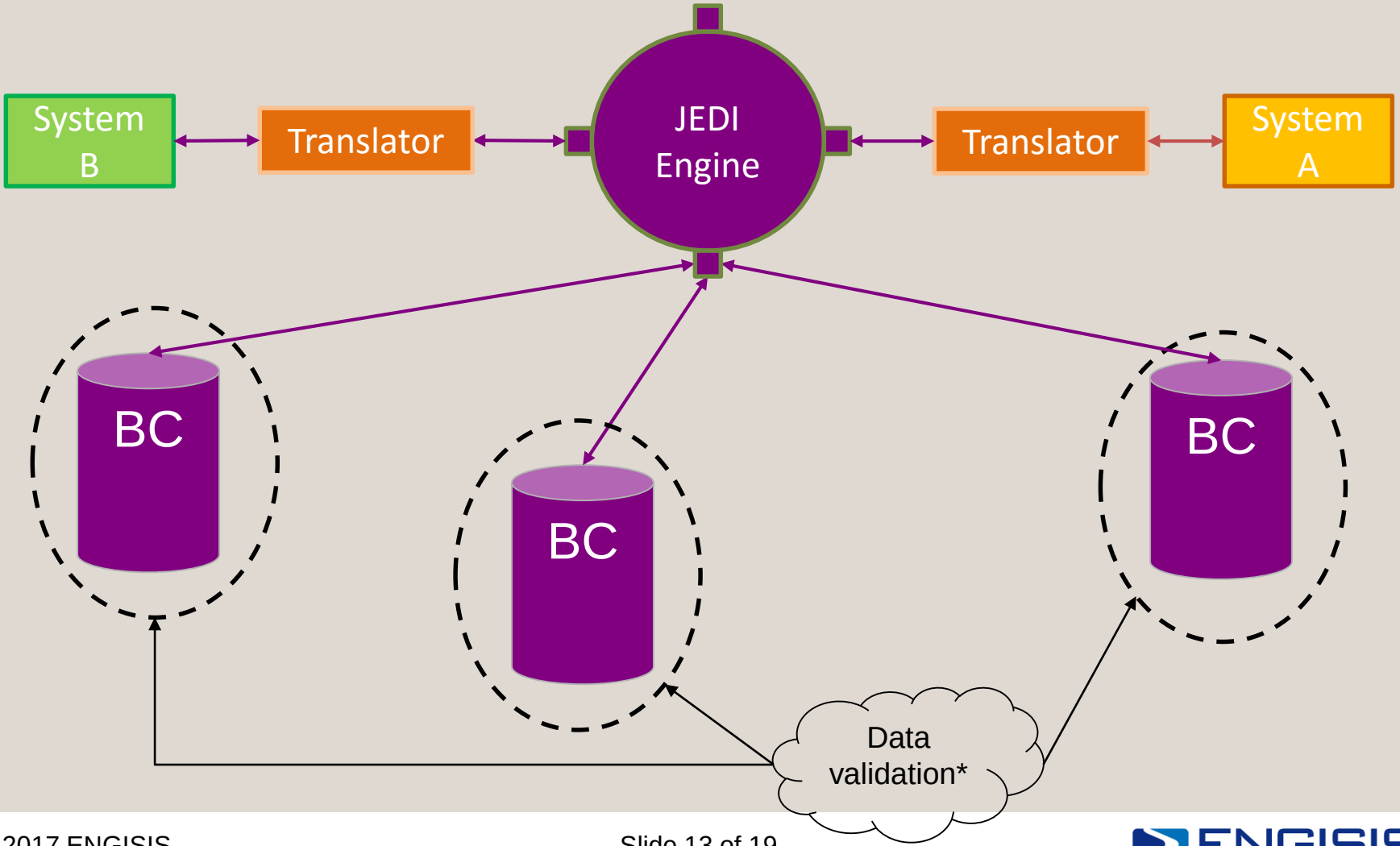
JEDI + Blockchain Potential Synergy

- JEDI data is stored using ISO 10303, open standard formats and metadata
  - High semantic quality for precise data context
  - Can increase the discovery, utility, and re-use of data in the Blockchain
  - No proprietary or legacy system formats
- Blockchain enhances integrity of data
  - Identifies the origin and timing of each transaction
  - Data can only be amended, not replaced
  - Consensus mechanism reduces/eliminates fraudulent data acceptance
- Technologies can be synergistic if both are applicable to the problem and solution

Generic JEDI architecture



Conceptual Architecture with Blockchain



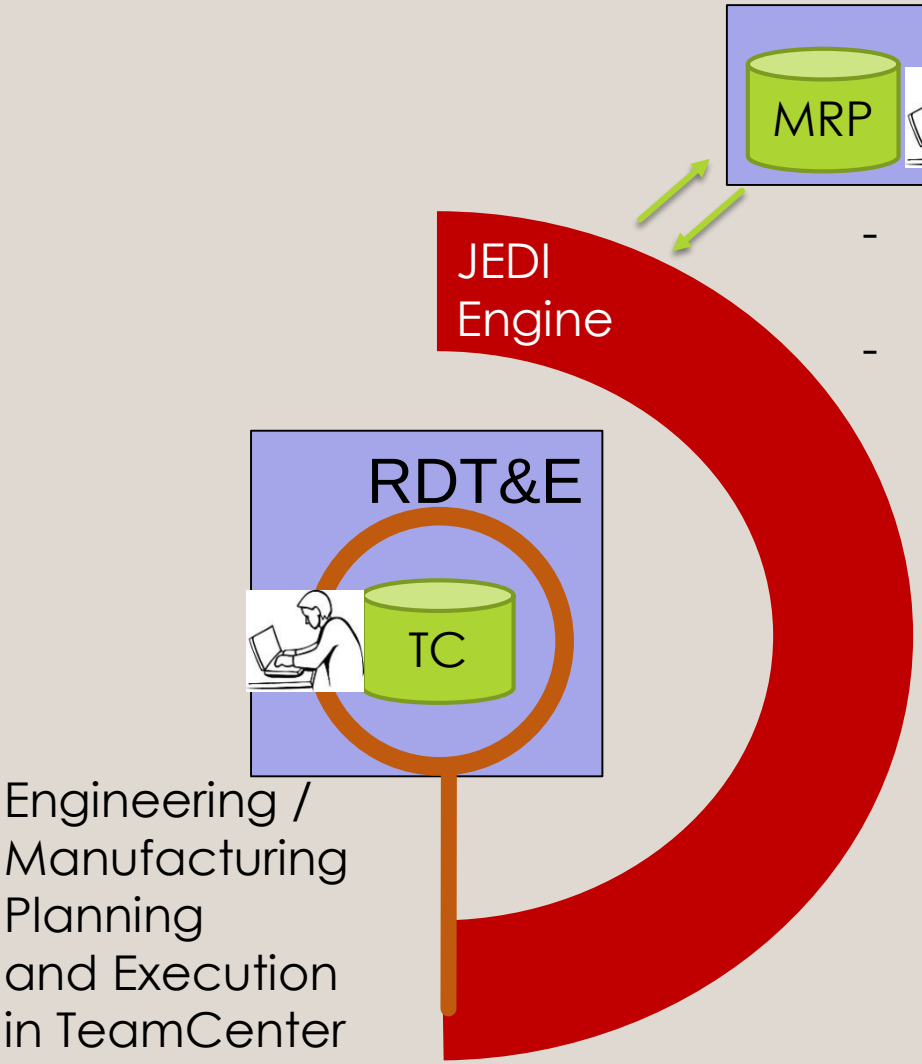
* Requires consensus before insertion

ENGISIS

Initial Blockchain Applicability Assessment

- Assessment simply made with G/Y/R circle
- Three areas assessed:
  - **Suitability** of Blockchain technology (Green best)
    - 2 or more User networks
    - Limited trust among Users
    - Able to capture transactions in Blockchain
  - **Value added** of Blockchain to project (Green best)
    - High value transactions
    - Demonstrated need for Blockchain data integrity
  - **Risk** adding Blockchain to JEDI Project (Green best)
    - Increased Blockchain scope causes risk to project objectives or timelines
    - Did not assess risk of project to Blockchain without knowing CIO goals

Applicability to JEDI IDSE: background



- Manufacturing Cost Estimate (MCE) metadata
- Feedback to Enterprise MRO scheduling in MRP

Applicability to JEDI IDSE

- Provide traceability of part requirement from identification in Depot induction, through digital manufacturing process
  - NAVAIR FRC East (MCAS Cherry Point, NC)
- JEDI deployed on DoD AWS Cloud to interact with information systems in NAVAIR RDT&E Network, and NextGEN (Former NMCI)
- Deployment awaiting concurrent FRCE migration to Teamcenter Product Data Management (PDM) suite
- Initial capability no earlier than Dec 2017

Suitability	Value	Risk
		

This work is sponsored by the National Institute of Standards and Technologies under Grant #70NANB15H093

Ongoing work

- Objective: storing in the chain the digital signatures and the fingerprint of the signed models (the facts)
- We prepared a test environment:
  - CentOS (https://www.centos.org/) virtual machines
  - Multichain (http://www.multichain.com/)
  - Using data streams (http://www.multichain.com/developers/data-streams/) to store and chain the facts
  - We will use multisignatures: before inserting a fact in the chain, I need the signature of N out of M members
- 1STEP : store on the chain a set of digital signatures generated from the DMC toolkit
- 2STEP: build a new tool that allows users to:
  - use the DMC toolkit to generate signatures that embed predefined metadata
  - notify users that they have been asked to authorize the insertion of a fact in the chain
  - add signatures to the multichain and attach custom metadata to ease retrieval
  - query the multichain to prove a signature exists

Risks and challenges with blockchain

- Technology is not mature
  - Lot of bugs
  - Few implementations
  - Fewer experts and tools
- No consensus about validation within the community itself
- Technology is limited
  - Data size
  - No real-time validation
- Implementations are expensive (power/energy)
  - To develop
  - To maintain
  - To run

Thanks. Questions?

Xenia Fiorentini
xenia.fiorentini@engisis.com