DECENTRALIZED AND AUTOMATED BUSINESS LOGIC IN A FUTURE MBSE BLOCKCHAIN ECOSYSTEM

ESA OSIP Project

Red Boumghar, Parametry.ai
Annalisa Riccardi, University of Strathclyde
Edmondo Minisci, University of Strahclyde
Ashwin Arulselvan, University of Strathclyde

MBSE22 Toulouse, France

DISCLAIMER

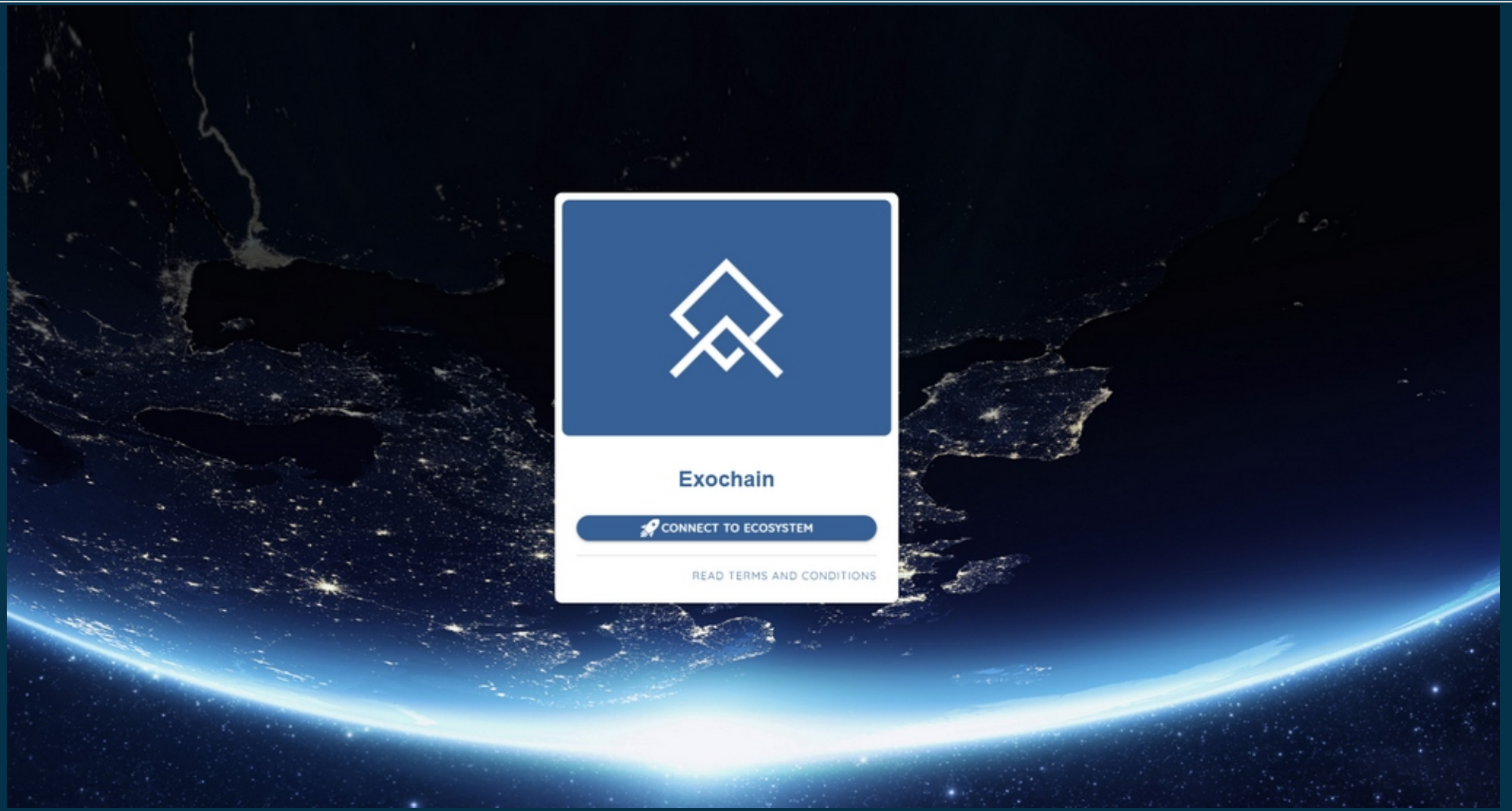
THIS IS NOT BITCOIN

THIS IS NOT A PUBLIC BLOCKCHAIN

THIS IS NOT ABOUT FINANCE

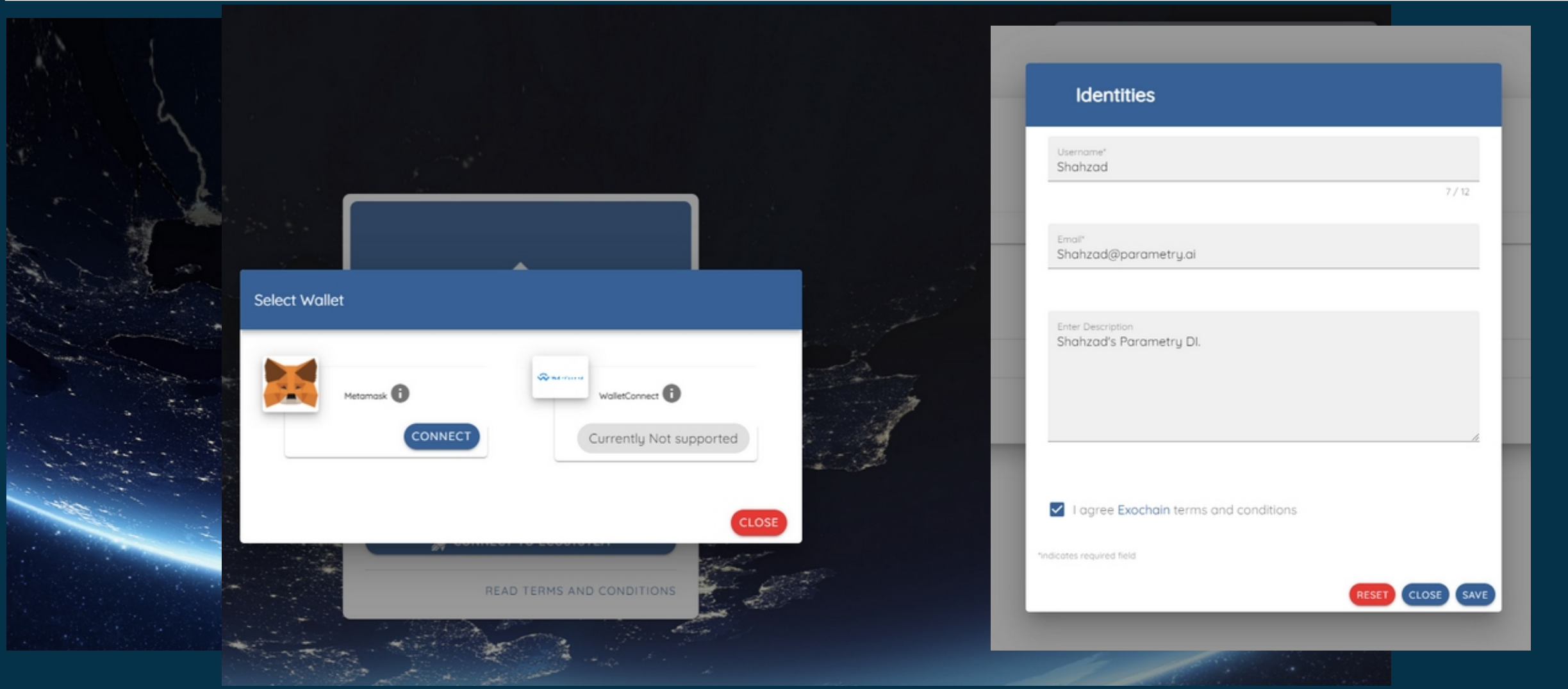
THIS IS ABOUT **TRUST** & **COLLABORATION**

Exochain: DApp – Web3 Prototype

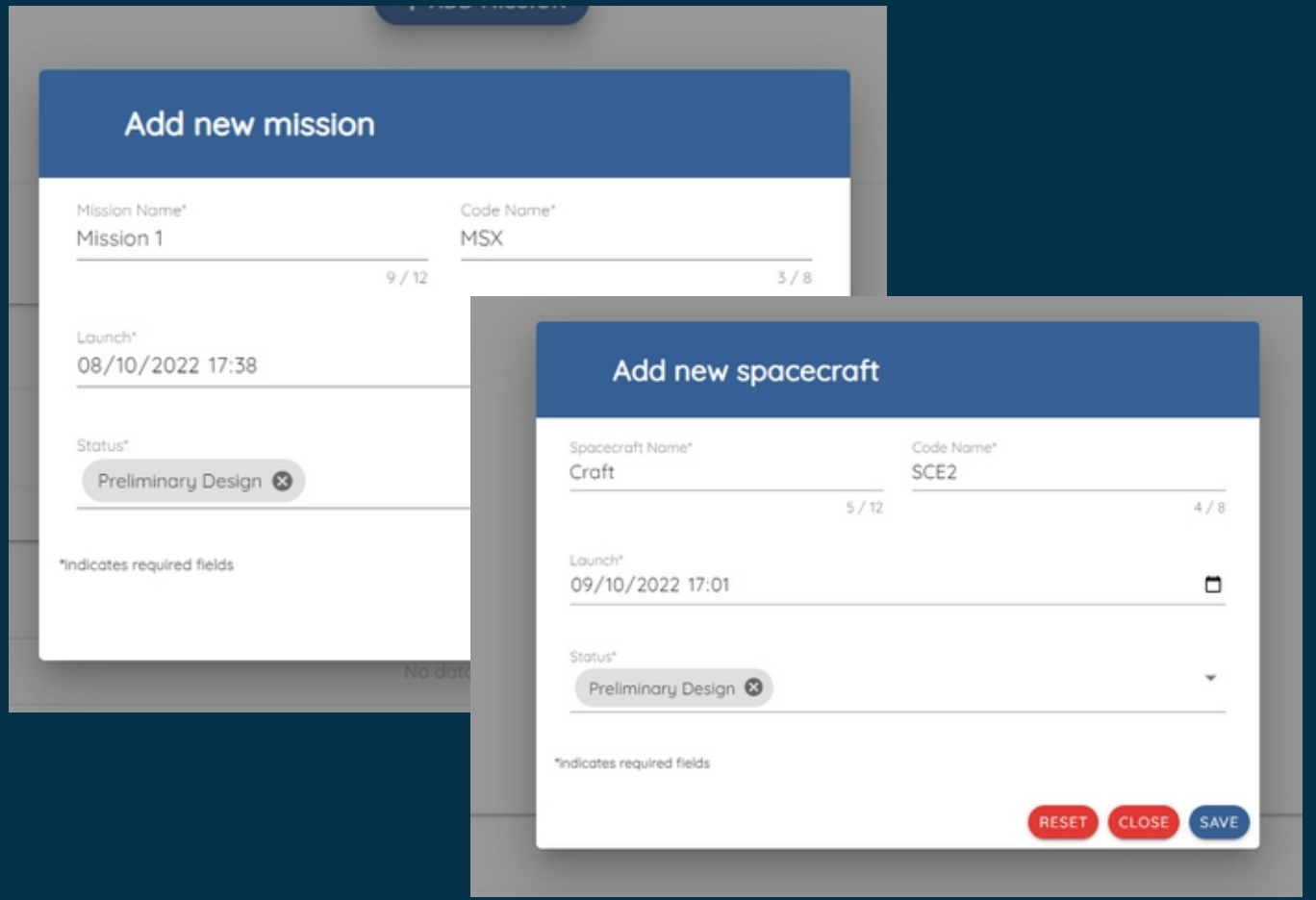


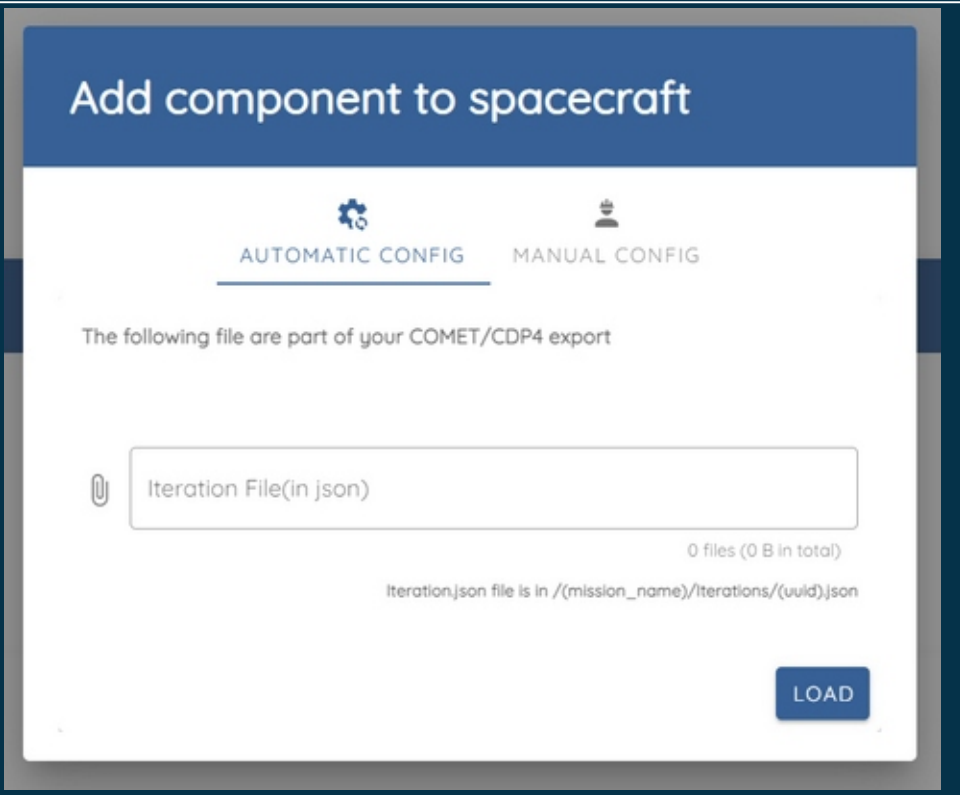
ESA OSIP Project: Distributed Ledger Technology for MBSE

Exochain: Decentralized Identity



Exochain: Decentralized Assets Management





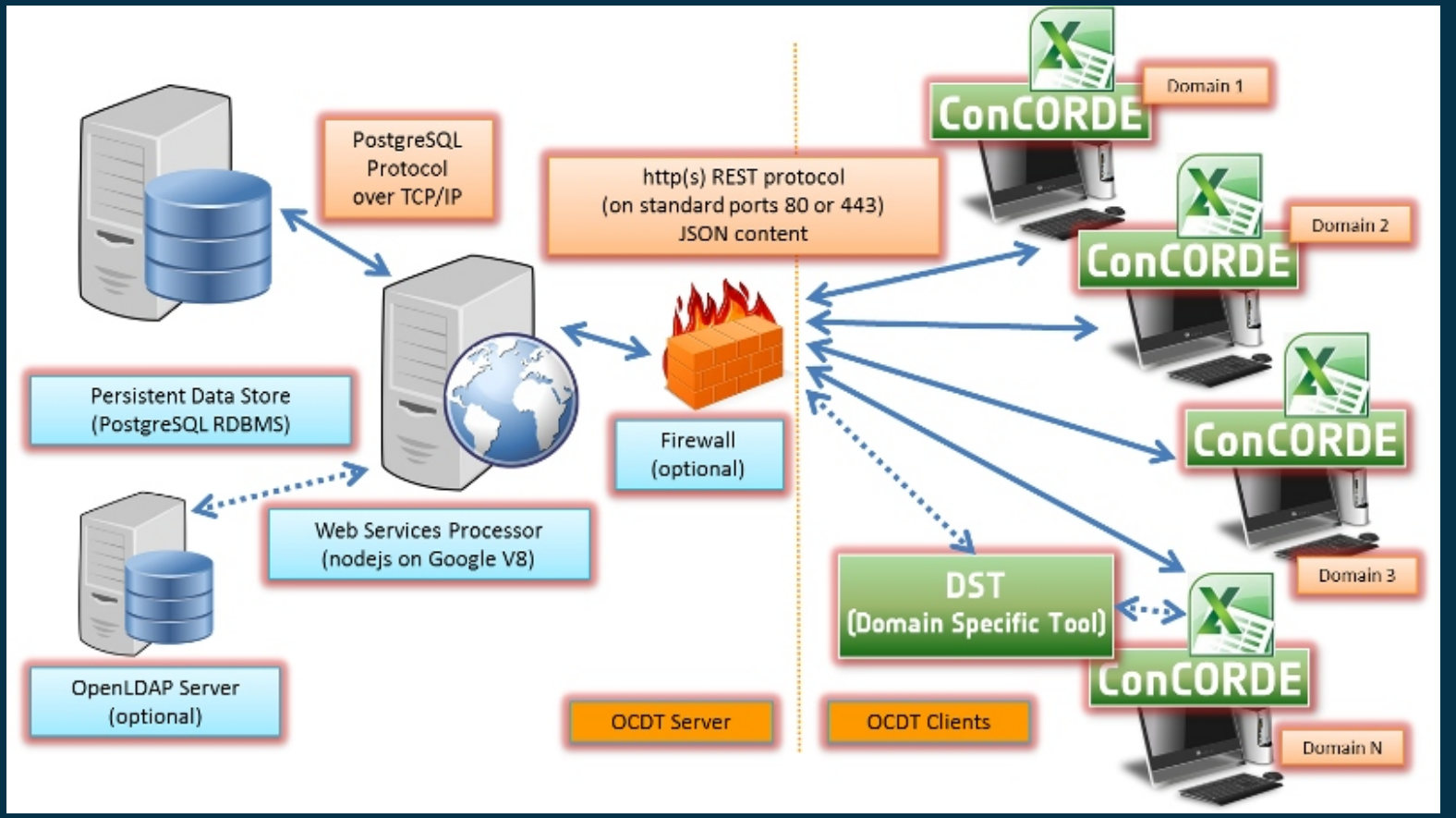
Automated Loading and Tracking of Assets And Identities

Need for decentralization & automation

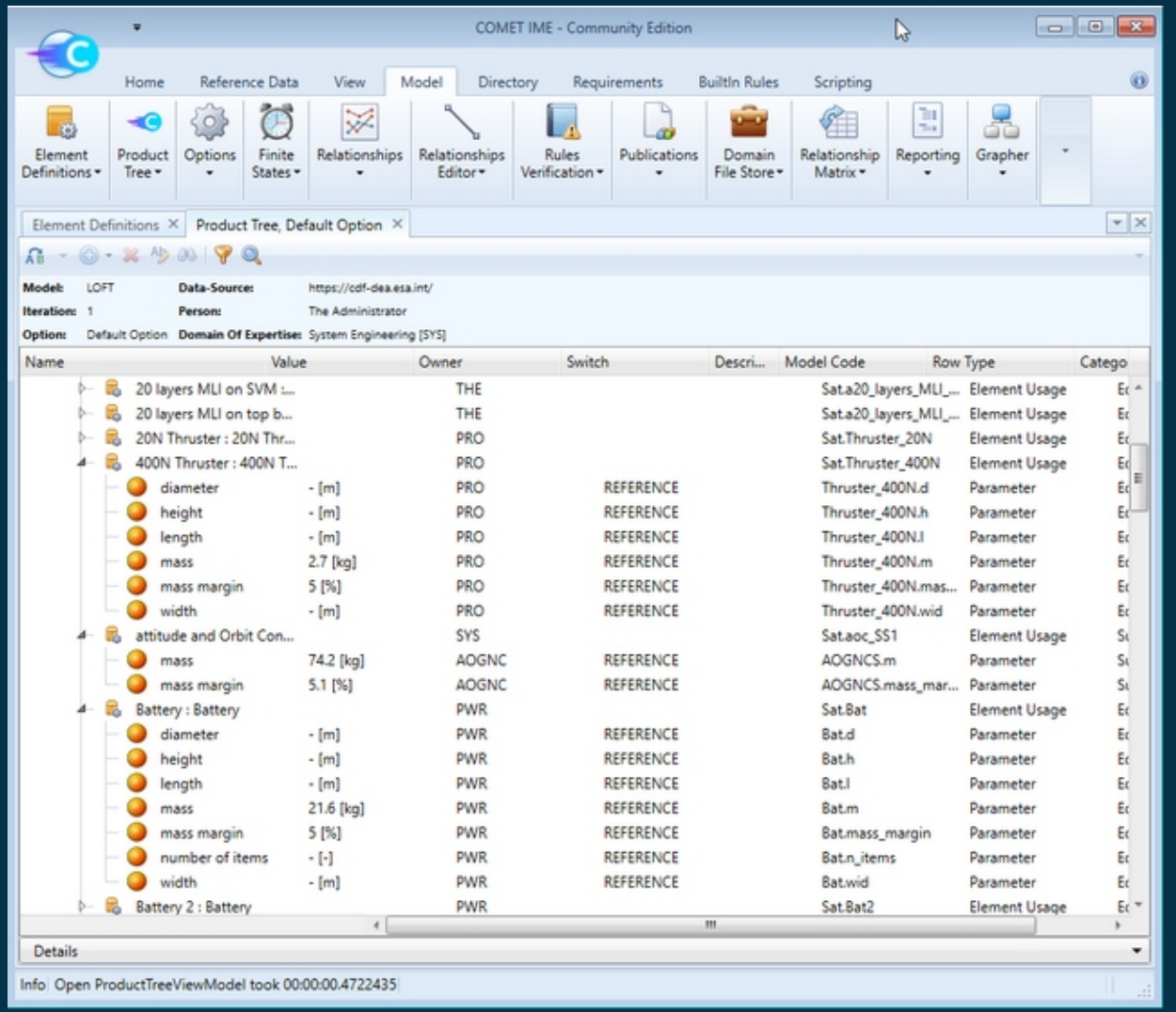
- Complex project
- Lots of Interactions
- Lots of stakeholders
- Lots of domain of expertise
- Lots of private/secret information
- Overload in mundane tasks for:
  - permissions and authentication management
  - Tracking, verifying, monitoring, auditing...

NEED FOR A **decentralized trusted partly-automated business network**

So we connected Excel sheets



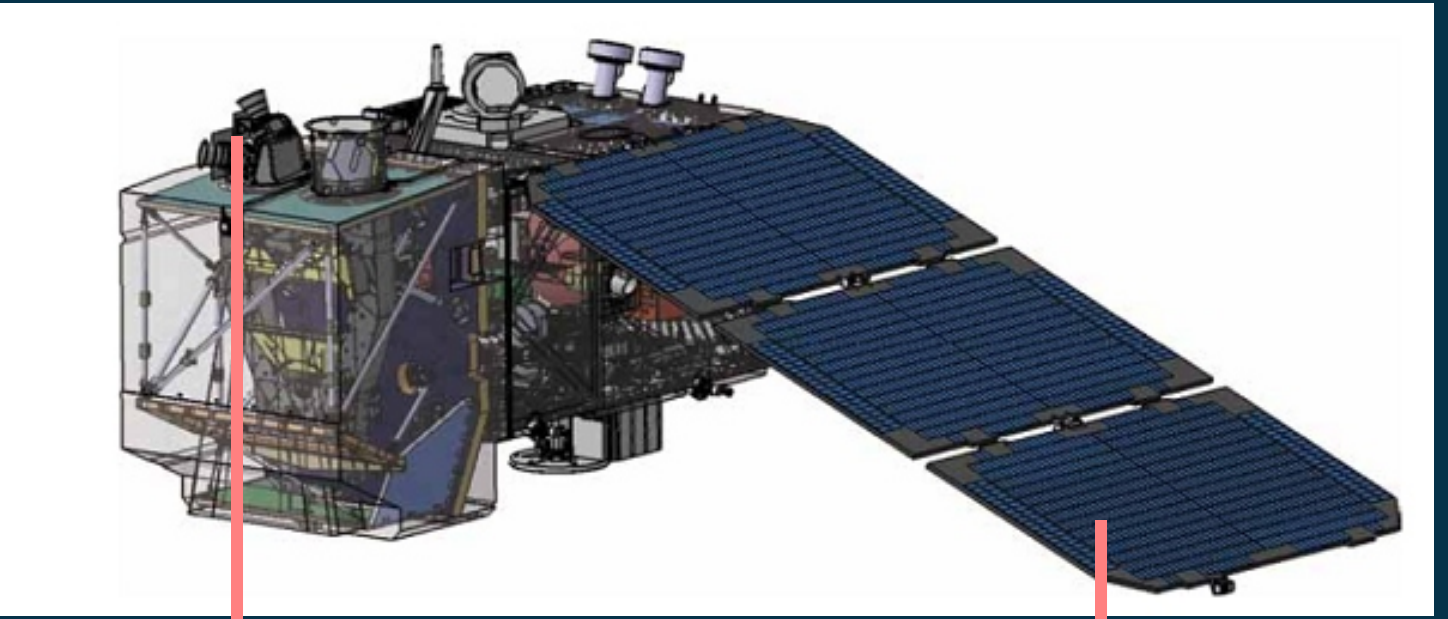
So we kept centralizing, with good access control



Exochain proposition

Exochain: event-based smart objects

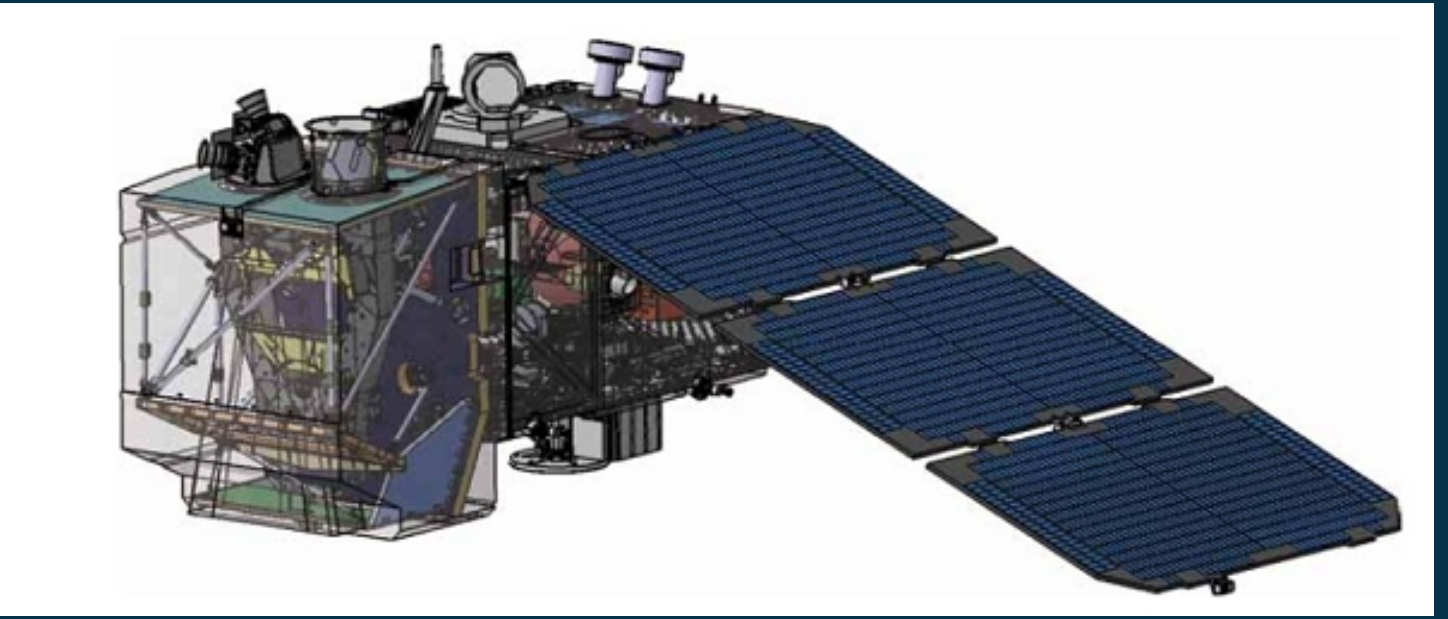
1 Smart Object
=
1 Small Program
Implementation



Star Tracker
- connects()
- estimates_attitude()
- takes_energy()

Solar Panel
- connects()
- collects_sun_rays()
- gives_energy()

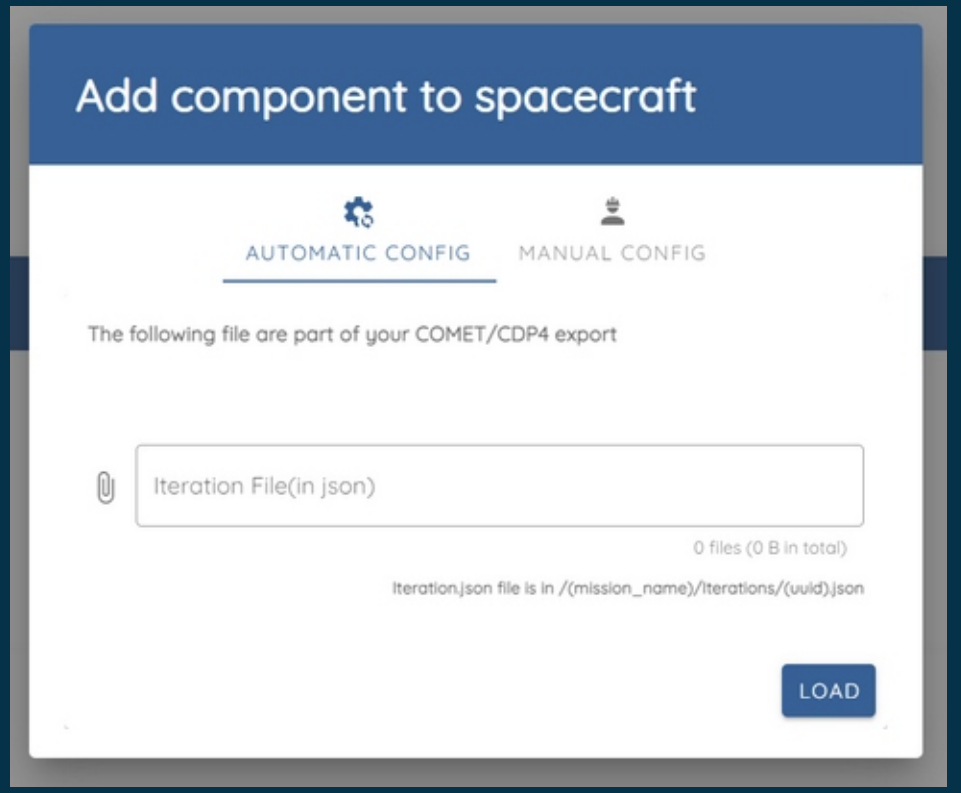
Exochain: event-based smart objects



smart objects ↔ external data sources

First Steps to Digital Twin

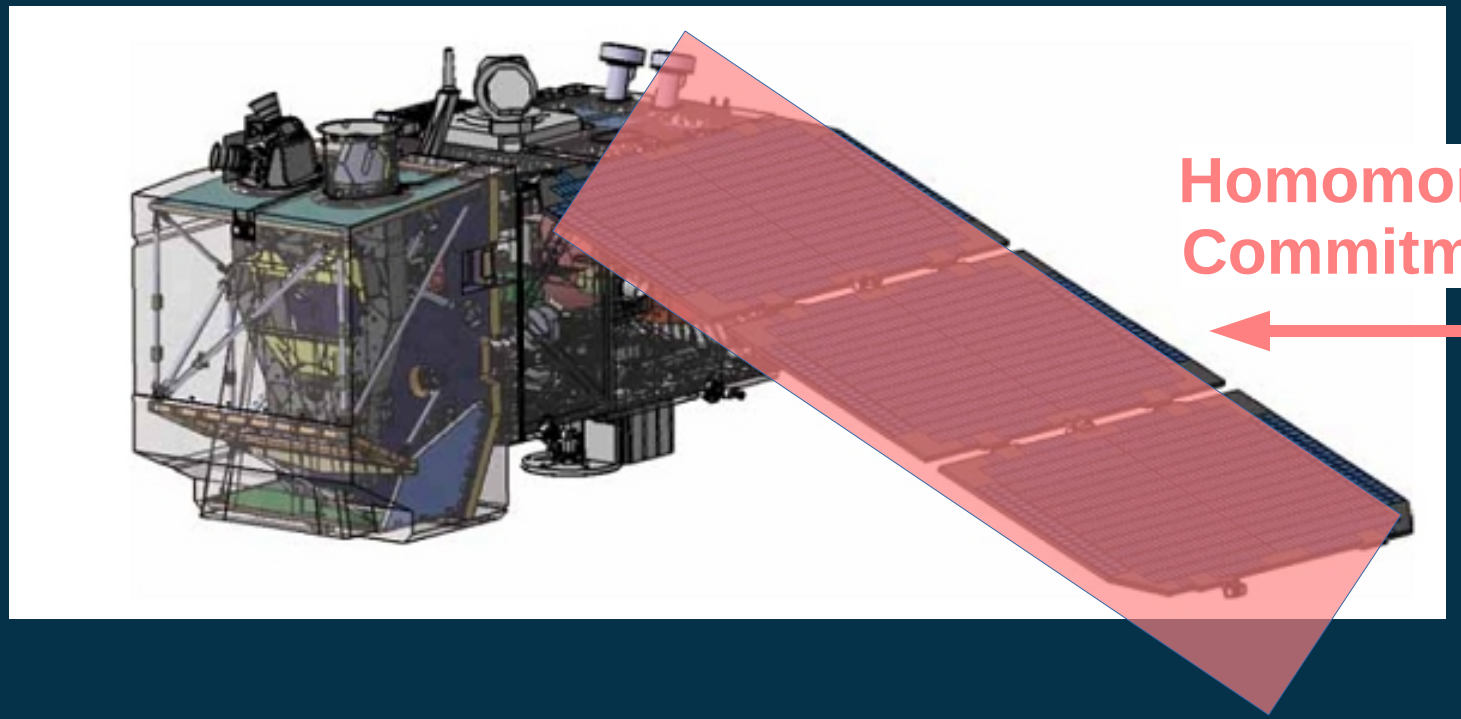
Exochain: Collaborating with Confidential Information



ZK-PROOF

Zero-Knowledge Proofs

Exochain: Collaborating with Confidential Information

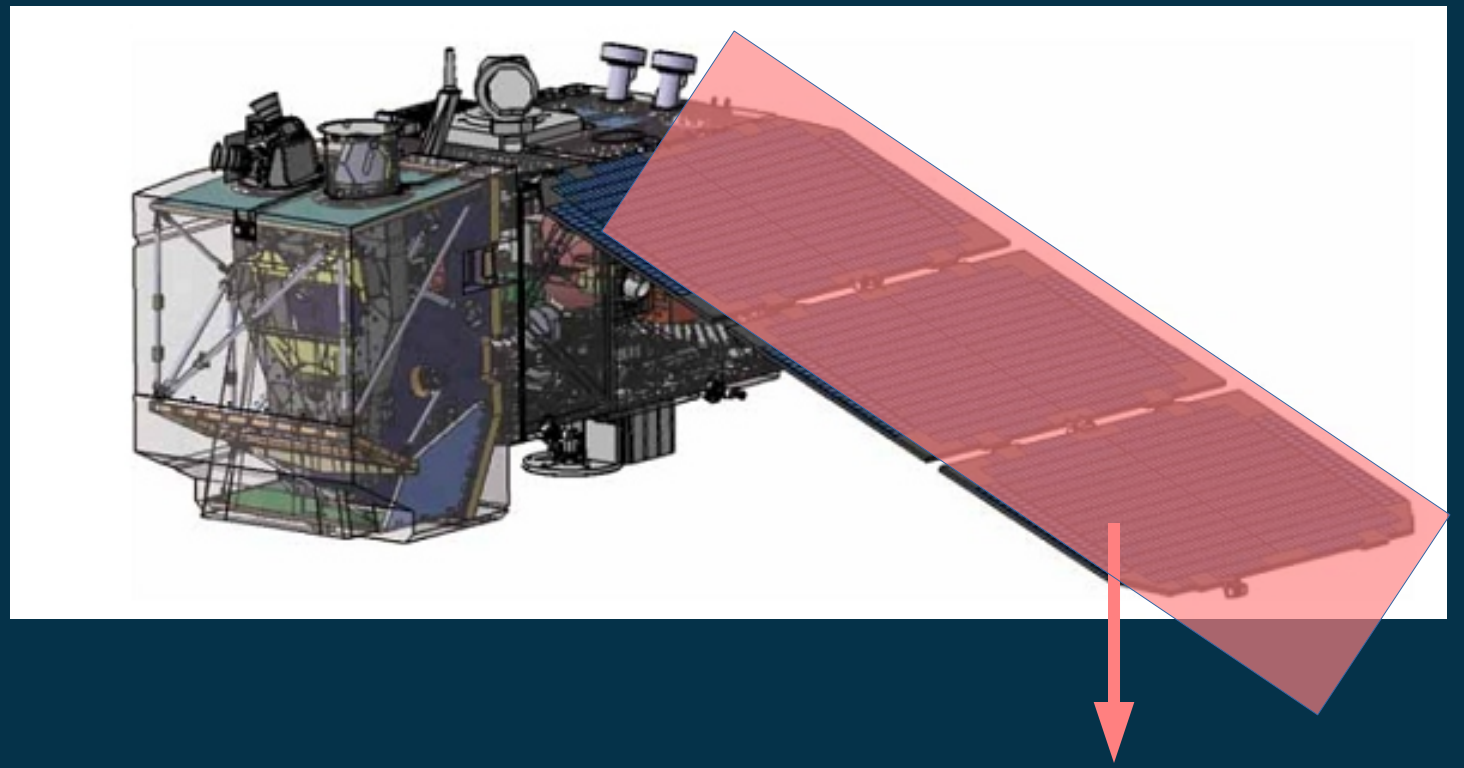


Homomorphic Commitments

ZK-PROOF

Zero-Knowledge Proofs

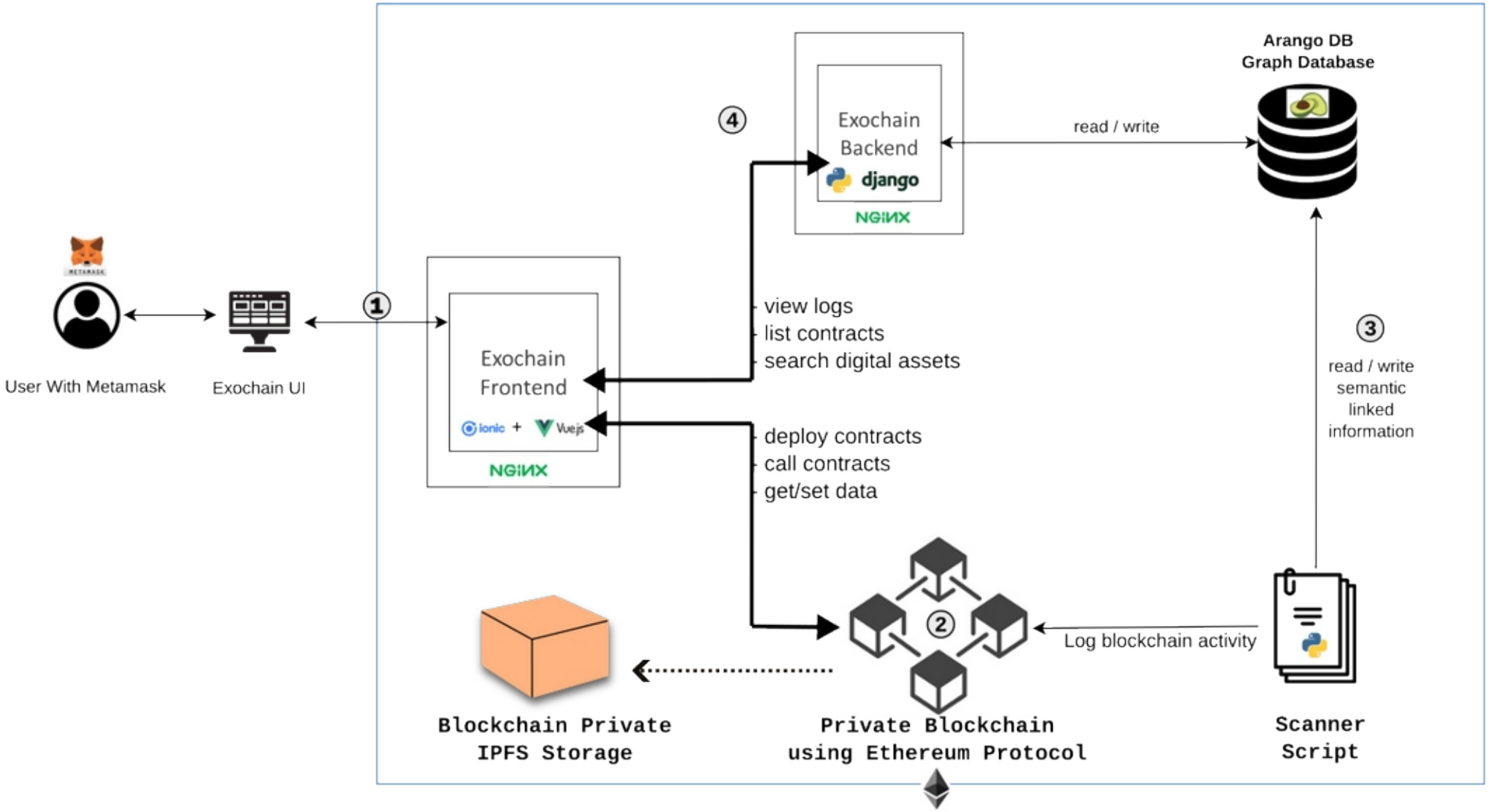
Exochain: Collaborating with Confidential Information



Solar Panel
- connects()
- collects_sun_rays()
- proves_it_can_give_enough_energy()

ZK-PROOF
Zero-Knowledge Proofs

Exochain: Architecture



Conclusion

- **Split by smart objects** forces decentralization
- **Decentralization** is haven to maintain **trust**
- **Smart Contracts** interactions and **ZK-Proof** permits automated interactions on confidential/secret information

Contact: red@parametry.ai

Conclusion

From a Technical Perspective

Blockchain is rarely easier or cheaper to set-up than modifying a traditional system

From a Trust Perspective

Blockchain can be easier and cheaper to set-up than a traditional system

Blockchain is a middleware to efficiently describe business logics

Composition of Blockchain Technology

Distributed Ledger

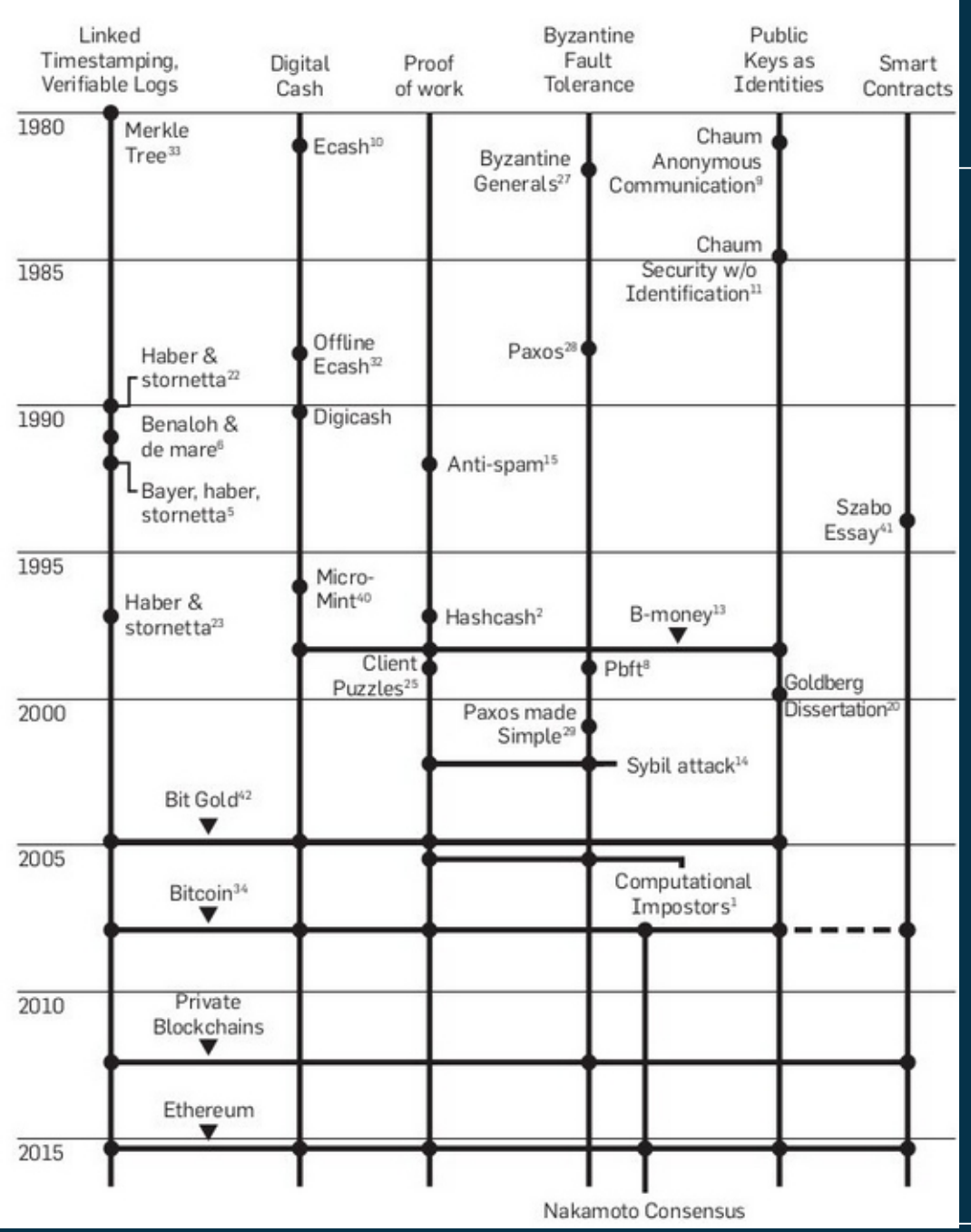
Transparent Information
Consensus on state of the whole system
Fault tolerance in distributed exchange

Encryption

Signing who is making the claim
Assertion of the origin

Chain history

Authenticity of history
Non-repudiation



Academic Pedigree of Blockchain Technology

"Bitcoin's academic pedigree", 2017
Naraynan & Clark
https://dl.acm.org/doi/10.1145/3132259