A Meta Model for Interoperability of Secure Business Transactions
Using BlockChain and DEMO

Sérgio Guerreiro[1,2], Wided Guédria[3], Robert Lagerström[4] and Steven van Kervel[5]
[1]*Instituto Superior Técnico, University of Lisbon, Av. Rovisco Pais 1, 1049-001 Lisbon, Portugal*
[2]*INESC-ID, Rua Alves Redol 9, 1000-029 Lisbon, Portugal*
[3]*1ITIS, Luxembourg Institute of Science and Technology (LIST),*
5 avenue des Hauts-Fourneaux, L-4362 Esch-sur-Alzette, Luxembourg
[4]*KTH Royal Institute of Technology, Sweden*
[5]*Formetis BV, Netherlands*

Keywords: BlockChain, Business Transactions, Security, Interoperability, Risk.

Abstract: Business transactions executed between organizations and individuals are largely operated on digital environments, conducting to an industrial interoperability challenge demanding secure environments to cooperate safely, therefore increasing credibility, and trust ability between end-users. This paper conceptualizes and prescribes a fine-grained control solution for the execution of business transactions involving critical assets, and using a human-based coordination and interaction design to minimize the negative impacts of security risks, the non-conformable operation and the coarse-grained control. This solution integrates the DEMO-based Enterprise Operating System (EOS) with BlockChain as a way to redesign, and distribute globally, a set of services that are founded in a human-oriented approach, and therefore, offering trust, authenticity, resilience, robustness against fraud and identification and mitigation of risk. The impacts for organizations and individuals are manifold: a security risk-based solution for end-users with budgetary constraints; educate on cyber security issues; and augment the trust for digital business processes environments.

1 INTRODUCTION

Nowadays, the business activities between companies and individuals, and companies with companies, for the production of new products and/or new services are often performed using electronic methods (Laudon et al., 2015), *e.g.*, e-services, electronic invoicing, e-payments, e-orders, *etc*. On the one hand, the stakeholders involved in a digital business transaction demand secure environments to interoperate safely, and therefore, increase the credibility and trustability between them. This requirement can also be substantiated by the multiple existing regulations, *e.g.*, Sarbanes-Oxley act (Act, 2002) or the EU General Data Protection Regulation (GDPR, 2017). On the other hand, there are many technological industrial solutions offering cyber security coverage at different layer of software systems, *e.g.*, access control model variants, encryption, tokens, firewalls, antivirus tools, *etc*. However, the implementation of these solutions are not easy accessible to Small and Medium Enterprises (SMEs), individuals, and public administration entities, due to technical complexity, high costs, demanding maintenance issues, *etc*.

The importance of this subject is emphasized by reports that *(i)* the cybercrime will cost businesses \$2 Trillion by 2019 (Security, 2015) and that *(ii)* the biggest concern of financial experts is a partial collapse of the financial system due to cybercrime activities. Some examples of industrial recognized problems are: *(i)* **collusion between procurement and suppliers** - enables the duplicate invoice payments to be made without the goods or services rendered to justify the second payment. Kickbacks are collaborative fraud example whereby a supplier submits an invoice that is inflated by the amount to be sent to the conspiring employee. Conflicts of interest can occur when an employee misuses their position to award contracts to suppliers for personal gain; *(ii)* **internal fraud**, are observed by phantom suppliers which is a set up of a new supplier on the electronic systems, and then, submitting false invoices for goods that are never delivered or services that are never provided. Check fraud, intercepting, or changing check on or-

Guerreiro S., GuÃ©dria W., LagerstrÃűm R. and van Kervel S.
A Meta Model for Interoperability of Secure Business Transactions - Using BlockChain and DEMO.
DOI: 10.5220/0006517502530260
In *Proceedings of the 9th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management (KEOD 2017)*, pages 253-260
ISBN: 978-989-758-272-1

ganization's bank account; and *(iii)* **external fraud or human error**, involve phishing with fake invoice, or claiming that invoice details have changed. Besides other factors, human errors are due to highly time-consuming and labor -intensive tasks required in the business transactions.

Moreover, organizations and individuals need to cooperate by the mean of communication and production to produce products and services. For example, the value chain upstream and downstream need to interoperate in order to minimize the bull-whip effect (Lee et al., 1997b) (Lee et al., 1997a). The aforementioned electronic invoicing and payments between organizations are examples of interoperability; which encompass responsibilities, such as, co-creation, co-production, contract, payments, *etc.* These concerns, add a social dimension to the problem of how to support an increased interoperability for secure business transactions between SMEs, local public administration, and individual citizens. Offering secure business transactions is not only a technological challenge, but rather a combination between social and technical dimensions.

Our position, is that it appears that world-recognized solutions such as Bitcoin and BlockChain are mainly devoted to the technological aspects (*e.g.*, Ethereum, Open Chain, Infosys, *etc.*), but, they pay little attention to the social dimension of humans performing business transactions in electronic networks of business transactions. Embedding the social dimension with the electronic business transactions augments the capability to contextualize the operation of organization in a business-oriented way. In fact, social dimension is natively present in all the business transactions executions: persons communicate, negotiate, *etc.*, to obtain their business intents. A digital business transaction solution cannot underestimate the social dimension as an important factor to the success of a technological implementation. Technology without social compatibility risks end-users resistance and abandonment.

This paper is organized as following. First, the background is introduced in terms of DEMO theory and methodology, interoperability and security. Then, the background work is synthesized in our position for future research. After that, the meta-model of the solution is presented. In the end, the conclusions and future work are discussed.

2 BACKGROUND

This section presents the key background concepts that are used to ground the position of our solution.

2.1 DEMO Business Transactions

As proposed in Enterprise Engineering (EE) (Dietz et al., 2013), a business transaction involves *(1)* actor role definitions, in order to specify who is responsible for each part of the transaction, who initiates it and who executes it, *(2)* a transition space definition, and *(3)* a state space definition. The state space is the set of allowable states of a system. The transition space is the set of allowable sequences of transitions of a system. State transitions are not dependent on their previous sequence or on the previous states but only on the actual one. When we refer to run-time business transactions, we are referring to the instances of the business transactions model that are executing at a precise and single instant in time. Many instances of a business transaction model could be executed at the same time in an organization. Following the Ψ-theory (Dietz, 2006), two distinct actor roles are identified in the standard pattern of a transaction: the Customer and the Producer. The goal of performing such a transaction pattern is to obtain a new fact. The transactional pattern, is performed by a sequence of coordination and production acts that produces a new service or product, encompassing three distinct phases: *(i)* the order phase with coordination and production acts of request (rq), promise (pm), decline (dc) and quit (qt), *(ii)* execution phase that includes production act of execution (ex) of the new fact itself and *(iii)* result phase that includes coordination and production acts of state (st), reject (rj), stop (sp) and accept (ac).

To increase security, business transactions ontologies are now being researched to accomodate the BlockChain (Gupta, 2017) concepts (de Kruijff and Weigand, 2017). In the near future, these solutions will be integrated with the operational environments where BlockChain is used, *e.g.*, private BlockChains.

2.2 Interoperability

Interoperability seems to be a straightforward concept. However, there is no common definition or shared comprehension of it. Each expert defines and understands interoperability, according to his domain. This led to the definition of the Ontology of Interoperability (OoI) (Naudet et al., 2010) formalizing the interoperability domain concepts. The OoI is based on the work of (Rosener et al., 2005), where a model for defining interoperability as a heterogeneous problem induced by a communication problem was proposed, and the Framework for Enterprise Interoperability (FEI) (Chen, 2006). The FEI was developed within the frame of INTEROP European Network of Excellence (NoE) (D. et al., 2007). The purpose of this framework is to define the research context of the interoperability and help identifying and structuring the knowledge in this domain. FEI defines a classification scheme for interoperability knowledge according to three dimensions: interoperability barriers, interoperability approaches, and enterprise interoperability concerns, also called enterprise levels. The OoI is mainly based on two models namely, the systemic meta-model which includes the resource composition model introduced by (Rosener et al., 2005) and the problem-solving meta-model, also called decisional meta-model. the systemic model describes systems as interrelated subsystems. A System is composed of SystemElement, which are systems themselves, and Relation. The Relation class formalizes the existing relationships inside a system, which is the source of the occurrence of interoperability problems. The problem-solving model is designed within a problem-solving perspective. Interoperability is implemented as a subclass of the Problem concept. Problems of interoperability exist when there is a relation, of any kind, between incompatible systems in a super- system they belong to or system they will form (i.e. a system to build). Incompatibility concept is a subclass of a more generic InteroperabilityExistenceCondition class aiming at explicitly formalizing the fact that Incompatibility is the source of interoperability problems for systems of any nature, as soon as they belong to the same super-system and there is a relation of any kind between those systems. Three kinds of interoperability problems are defined in FEI (Chen, 2006): conceptual (i.e. mainly concerned with the syntactic and semantic incompatibilities), technological (i.e. refer to the use of computer or ICT) or organizational (i.e. relate to the definition of responsibilities and authorities). Solutions solve problems and can in turn induce new problems. Two kinds of solutions, namely *a priori* and *a posteriori* solutions are defined, with respect to the occurrence of the problem. Solutions solving problems by anticipation are *a priori* solutions. *A posteriori* solution can be used for solutions correcting problems after they occurred. These solutions may follow one of the following approaches, as defined in the FEI: a) Integrated approach (i.e. characterized by the existence of a common format), b) Unified approach (i.e. characterized by the existence of a common format but at a meta-level), c) Federated approach (i.e. no common format is defined)

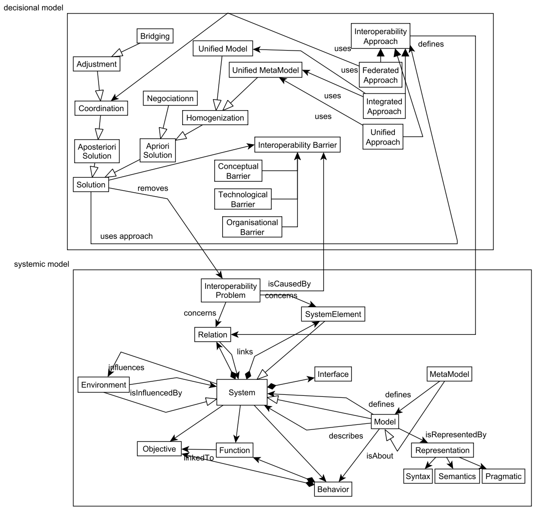

Figure 1: Extract of the OoI metmodel.

2.3 Security

The interconnected digital world brings enormous benefits, but it is also vulnerable. For commercial entities that depend on the digital world for their everyday business activities, this means added uncertainty. Antagonistic or non-antagonistic information technology incidents could end up harming or destroying the business. Also, the interplay between technology and business operations in modern enterprises is becoming increasingly complex. Organizations need to utilize their assets in best possible ways in order to fulfill their missions. The complexity and security issues come hand in hand today. The more complex the business and its technology is the more vulnerable you are to attacks. As an enterprise you need to make sure the whole attack surface is secured, while the attacker only needs to find one vulnerability in order to get in. Unfortunately, today there are few tools and approaches helping with this. Most available methods are reactive or very limited in scope.

In order to be proactive and cover the whole attack surface a holistic approach that also include technical details is needed. The few tools available that say they cover this area are however driven by manual labor and require a high level of security expertise, which is both expensive and hard to come by. A research initiative from KTH Royal Institute of Technology however aims to cover this gap by developing pwnPr3d (Johnson et al., 2016a) (Johnson et al., 2016b), an attacker-centric threat modeling technique for automated threats identification and quantification based on network modeling. Instead of relying on human expertise to analyze a model and decide whether it is secure or not, and where the key flaws in the architecture are located, pwnPr3d automatically performs this analysis. That is, the security expertise is built into the model. In its analysis, pwnPr3d generates probability distributions over the Time To Com-promise (TTC) for each asset in the system. An important aspect of pwnPr3d is that it has been designed as a closed meta-modeling architecture, similarly to MOF, with layers of increasingly concrete sub languages. It makes pwnPr3d highly flexible in terms of introducing new types of ICT assets and vulnerabilities. Also, an object-oriented structure provides support for information, encapsulation and separation of concerns, thereby reducing complexity for all stakeholders, regardless of the level of detail they require. It also promotes reusability of model elements using component libraries to store standard components such as specific network stacks, firewalls or operating systems.

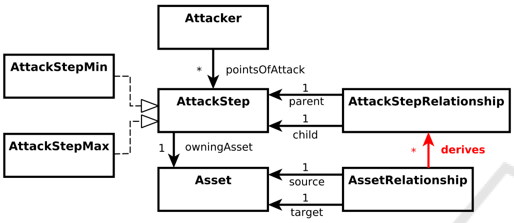

Figure 2: Layer-0 of the pwnPr3d metamodel.

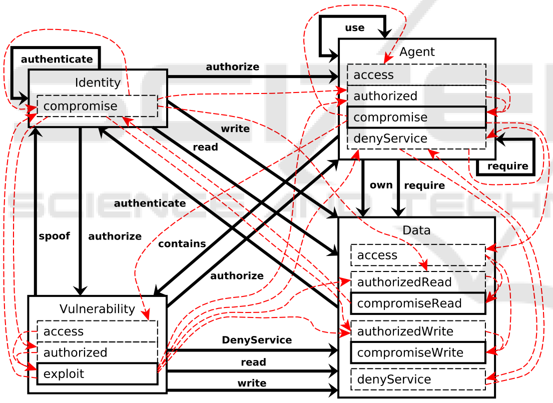

Figure 3: Layer-1 of the pwnPr3d metamodel.

In Figure 2 we present what we call Layer-0 of the pwnPr3d metamodel. The main purpose of Layer-0 is to couple the components of an IT infrastructure and the attack surface of the attacker. It defines the attack graph theory, *i.e.* the possible progression of the attacker through attack steps, as well as TTC calculation. In the figure 3, Layer-1 is presented. Layer-1 introduces the network and system-specific logic for the attack graph generation, the various threat types that can be identified in a network, and loss calculation from CIA breaches. It uses Layer-0 as a metamodel and all the classes introduced in this layer are instances of the Asset entity, and each Asset instance contains its own set of attack steps.

Authorization and its enforcement (access control) have been a crucially important pillars of enterprise information technology security, both on a technical level (in computer systems, databases, networks, *etc.*) and an organizational level (access policy and its human enforcement). In parallel to their role in IT and IT architectures, authorization and access control are essential in physical premises such as airports and industrial facilities, thus it is easy to imagine the importance of authorization and access control being functioning appropriately and being well-aligned with the enterprise. However, as with security in general authorization has also been poorly managed. In our approach, proposed in this paper, we aim to further develop and make us of the threat modeling framework of pwnPr3d and align it with current modeling and analysis standards in authorization and access control for complex systems (Korman et al., 2016).

2.4 Co-creation and Co-production in Production Chains

Co-creation and Co-production in production chains is the typical way of cooperation one observes in many high value industrial production chains such as finance, automotive, *etc*. Instead of well-defined products directly available from stock, companies - contractors - that are part of virtual enterprise chains propose to develop custom-made products within a clearly defined domain of their competences and well-matching the specific needs of the customers - principals. Once the product and the matching price conditions are well specified, parties may sign a contract. During the life time of the contract parties order productions and request matching payments.

In (Hunka et al., 2016) and (Hunka and van Kervel, 2017) a generic DEMO model is proposed for co-creation and co-production in industrial production chains.

As depicted in Figure 4, the co-creation phase where parties seek a shared understanding of the production to be delivered, and the price that may have to be paid is represented by transaction T1 and T2 (T1.accept and T2.accept). Note that this shared understanding is represented by two 'documents' but does not yet imply a legally binding contract to deliver products at the price specified. The two documents represent an unsigned contract. Parties may or may not agree to sign this contract. They may decide to re-exececute the co-creation phase, resulting in a new product specification and matching price conditions. The signing of the contract is represented by two DEMO transactions T3.promise and T4.promise.

In the co-production phase parties order the production and request the matching payments, as stipulted by the signed contract. Each delivery and pay-

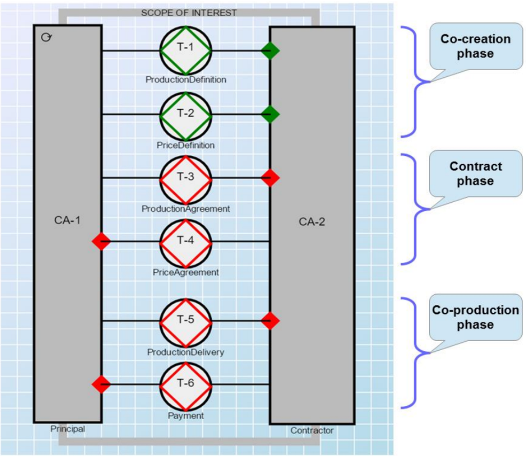

Figure 4: CC-CP DEMO model.

ment is an instance of T5 and T6 (T5.accept and T6.accept).

At the end of the life time of the contract parties assess whether the contract has been fulfilled well by both parties and the contract is terminated. This is represented by T3.accept and T4.accept.

There exist many business rules, represented by the DEMO PM and AM models. For example; ”pay first”, and ”deliver after receipt of payment”, or vice versa. T1.accept and T2.accept is a condition that must be met before T3.request and T4.request can be issued. T5.request and T6.request can be issued only after T3.promise and T4.promise. It is assumed - to be validated by appropriate case studies - that the expressivity of the CC-CP model is ontologically complete. Meaning that any imaginable business case is well captured and executable.

The CC-CP modelis devised to meet the following objectives and requirements: i) Governance, defined here being the system and ways by which companies are directed and controlled. In virtual co-creation and co-production enterprises this is mostly defined by the contract(s) devised and signed by the constituting enterprises. ii) Risk, the application of methodologies through which parties identify, analyze, prioritize, define and mitigate risks that affect the interests of stakeholders. iii) Compliance, defined being the overall approach through which an operation of the parties conform with stated requirements from outside the enterprise, such as legal regulations and moral rules. Notably the banking crisis resulted in extensive complex regulations such as Sarbanes-Oxley Act (Act, 2002) that must be implemented by banks. iv) Efficiency, the careful use of precious resources to realize the desired results. v) Effectiveness, the degree of how well the requirements of the principal are met; a degree for quality. vi) Agility, the capability to adapt the operation of an enterprise at any time, driven by unpredictable changes in markets, imposed legislation and strategy.

The CC-CP model is ontological, and implementation-independent. For any real-world implementation specific transactions and AM rules must be modeled. The CC-CP model is considered - to be proven empirically - the generic and appropriate implementation-independent DEMO model for the analysis of Risk and secure transactions.

3 POSITION PROPOSAL

Our proposal aims at increasing the trustability between the stakeholders and users of a business processes execution environment. Where a business processes execution is a complex interchanges of communication and production acts. The referred pattern of Co-creation and Co-production in production chains is a classical example of such a complex interaction. To reach that end, we propose to raise the transparency of the running business processes using a richer design (ontological based) concerning Security, Interoperability and Control.

Enterprise Operating System (EOS) (Guerreiro et al., 2013) is a Model-driven environment software system that is founded in the Ψ-theory from the DEMO theory and methodology (Dietz, 2006) (Dietz et al., 2013). EOS allows an agile implementation of the software systems supporting the business processes operation.

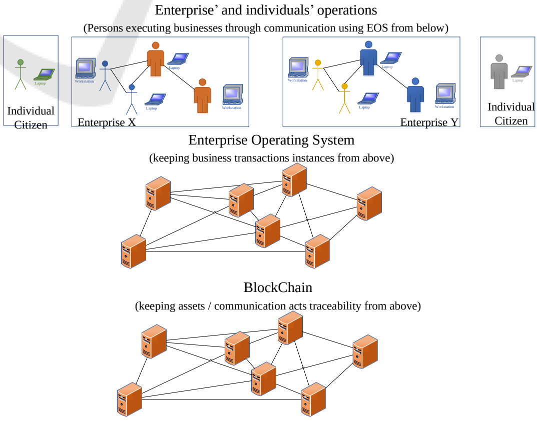
Enterprise' and individuals' operations
(Persons executing businesses through communication using EOS from below)
Individual Citizen
Enterprise X
Enterprise Y
Individual Citizen
Enterprise Operating System
(keeping business transactions instances from above)
BlockChain
(keeping assets / communication acts traceability from above)

Figure 5: Enterprise Operating System offering business processes run-time execution to multiple stakeholders and supported by a private BlockChain.

EOS integrated with BlockChain (Gupta, 2017), *cf.* the free-hand schematics in Figure 5, will increase the trust between end-users, and conversely the cyber security awareness increases between them allowing the operation of more business transactions. In specific the integration allows the following benefits. Business transactions operation **not conformable with prescriptions**: end-users have an active and independent role in the execution of business transactions; therefore, it does not guarantee that the security requirements of business transactions are met properly on their daily routines. For example, if a company's recommendation to always obtain a written record when contacts are made with clients, nothing limits the ability of an end-user to contact a client directly, by phone, without leaving any trace of the communication made to the other actors the same organization. **Fine grained** access control, in oposition to the usual coarse-grained control of critical assets or establishing few control points during the execution of business transactions drives to black holes where the asset traceability is lost. This phenomenon is observed in the financial markets, with a huge adverse impact potential to the organization and to its environment.

4 META-MODEL DESIGN

Figure 6 defines a meta model for the interoperability of Secure Business Transaction, using ArchiMate specification language (Group, 2017). Clear responsibilities of initiating and executing business transactions are assigned to the business actors of each company. Then, the run-time control of business transactions execution is performed by the Enterprise Operating Systems at the application level. A meta model is equivalent to the conceptual approaches concerning security and business transactions, *e.g.*, (Gaaloul et al., 2014).

The concept of ArchiMate *business service* is realized by the concept of *business transaction*. The *business roles* are assigned to the *business transaction*. And, the *business actors* are assigned to the *business roles*. In practice, these associations represent the organizational model definitions using DEMO.

The application counterpart of the *business transaction* is served by the *Enterprise Operating System* application service, which is able to execute directly the DEMO organizational models. It is composed by an *application component*. When a change in the state of a business transaction is required, then *pwnPr3d* application component is used. *PwnPr3d* is responsible to control the access to the *business transactions states* data objects. The concepts grouped by the tag "meta-model for interoperability of Secure Business Transaction" (concepts in the middle of the Figure 6) could be enforced by any of the participating companies or by any third party.

To guarantee the trust ability between all the involved companies a private BlockChain is used. All the changes performed by the Enterprise Operating System, and that are cumulatative granted by pwnPr3d, are immutably published in the private BlockChain network, allowing all the involved business actors to consult transparently all the business transactions performed.

5 CONCLUSIONS AND FUTURE WORK

This paper addresses the conceptual integration between three research areas: business transations model and execution; security and interoperability. The challenge is to find a solution for the open problem of companies that are included in complex value chains demanding co-operation to succed in their business processes. It is commonly agreed that security is required to avoid unauthorized accesses risks such as access to classified information and data. Security area offers many solutions to this problem. Yet, the lack of trust between companies could be a barrier for making new business. In this sense, BlockChain seems a solution that allows a transparent way of operating business processes. Any of the involved is able to consult the chain and check the validity of other's actions. Moreover, business transactions are not only mechanical actions performed by machines. In reality, people are always communicating and producing artifacts. Enterprise Operating System (based on DEMO) is by nature a solution that deals with the Human communication and that is able to orchestrate the interactions while business transactions execute. Social dimension is natively present in all the business transactions executions: persons communicate, negotiate, *etc.*, to obtain their business intents. A digital business transaction solution cannot underestimate the social dimension as an important factor to the success of a technological implementation. Technology without social compatibility risks end-users resistance and abandonment.

Our position, is presented as a meta model using ArchiMate specification language, integrates the areas of business transations model and execution; security and interoperability. Future research in terms of meta model validation and implementation is derived.

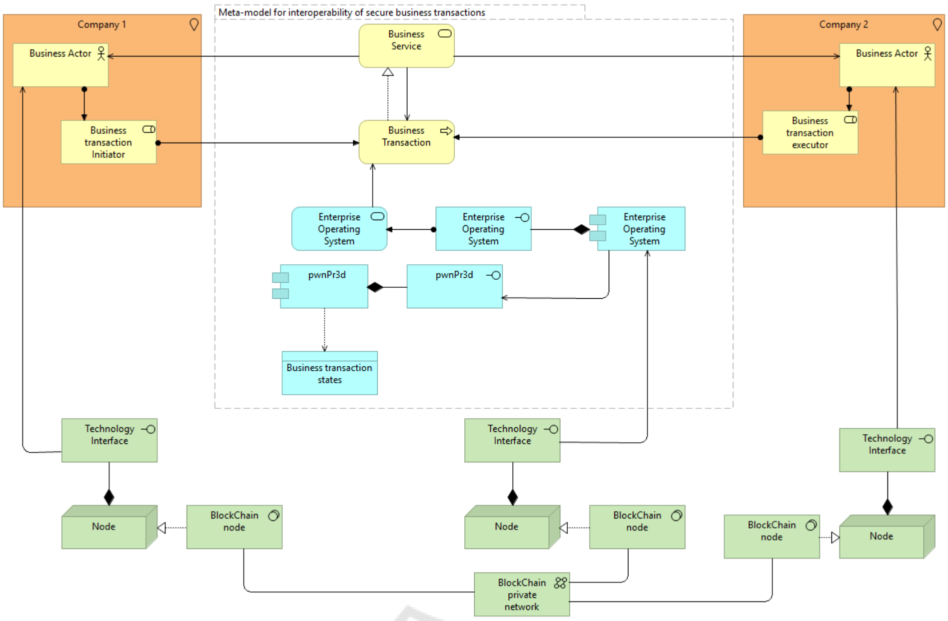
Meta-model for interoperability of secure business transactions
Company 1
Business Actor
Business transaction Initiator
Business Service
Business Transaction
Company 2
Business Actor
Business transaction executor
Enterprise Operating System
Enterprise Operating System
Enterprise Operating System
pwnPr3d
pwnPr3d
Business transaction states
Technology Interface
Technology Interface
Technology Interface
Node
BlockChain node
Node
BlockChain node
BlockChain node
Node
BlockChain private network

Figure 6: A Meta Model for interoperability of Secure Business Transaction.

ACKNOWLEDGEMENT

This is a collaboration work between different institutions. Part of this work is supported by national funds through Fundação para a Ciência e a Tecnologia (FCT) with reference UID/CEC/50021/2013; and conducted in the context of the PLATINE project (PLAnning Transformation Interoperability in Networked Enterprises), financed by the national fund of research of the Grand Duchy of Luxembourg (FNR), under the grant C14/IS/8329172.

REFERENCES

Act, S. (2002). Sarbanes-oxley act. pub.l. 107-204, 116 Stat. 745, enacted July 30.

Chen, D. (2006). Enterprise interoperability framework. In *EMOI-INTEROP*.

D., C., M., D., and B., E. (2007). Interop noe deliverable di.3: Enterprise interoperability framework and knowledge corpus - final report. Technical report, Interoperability Research for Networked Enterprises Applications and Software (INTEROP Network of Excellence), IST - Contract no.: IST-508 011.

de Kruijff, J. and Weigand, H. (2017). *Understanding the Blockchain Using Enterprise Ontology*, pages 29–43. Springer International Publishing, Cham.

Dietz, J. L., Hoogervorst, J. A., Albani, A., Aveiro, D., Babkin, E., Barjis, J., Caetano, A., Huysmans, P., Iijima, J., van Kervel, S., et al. (2013). The discipline of enterprise engineering. *International Journal of Organisational Design and Engineering*, 3(1):86–114.

Dietz, J. L. G. (2006). *Enterprise Ontology: Theory and Methodology*. Springer.

Gaaloul, K., Guerreiro, S., and Proper, H. A. (2014). Modeling access control transactions in enterprise architecture. In *Business Informatics (CBI), 2014 IEEE 16th Conference on*, volume 1, pages 127–134. IEEE.

GDPR (2017). Eu general data protection regulation. http://www.eugdpr.org/.

Group, O. (2017). Archimate® 3.0 specification. Open Group Standard, http://pubs.opengroup.org/architecture/archimate3-doc/.

Guerreiro, S., van Kervel, S., and Babkin, E. (2013). Towards devising an architectural framework for enterprise operating systems. In *8th International Conference on Software Paradigm Trends (ICSOFT-PT 2013)*, pages 578–585. INSTICC.

Gupta, M. (2017). *Blockchain For Dummies ®, IBM Limited Edition*. John Wiley & Sons, Inc.

Hunka, F. and van Kervel, S. J. (2017). The rea model expressed in a generic demo model for co-creation and co-production. In *Enterprise Engineering Working Conference*, pages 151–165. Springer.

Hunka, F., van Kervel, S. J., and Matula, J. (2016). Towards co-creation and co-production in production chains modeled in demo with rea support. In *Enterprise Engineering Working Conference*, pages 54–68. Springer.

Johnson, P., Vernotte, A., Ekstedt, M., and Lagerström, R. (2016a). pwnpr3d: an attack-graph-driven probabilistic threat-modeling approach. In *Availability, Reliability and Security (ARES), 2016 11th International Conference on*, pages 278–283. IEEE.

Johnson, P., Vernotte, A., Gorton, D., Ekstedt, M., and Lagerström, R. (2016b). Quantitative information security risk estimation using probabilistic attack graphs. In *International Workshop on Risk Assessment and Risk-driven Testing*, pages 37–52. Springer.

Korman, M., Lagerström, R., and Ekstedt, M. (2016). Modeling enterprise authorization: A unified metamodel and initial validation. *Complex Systems Informatics and Modeling Quarterly*, (7):1–24.

Laudon, K. C., Laudon, J. P., et al. (2015). *Management information systems*. Pearson Upper Saddle River.

Lee, H. L., Padmanabhan, V., and Whang, S. (1997a). The bullwhip effect in supply chains. *Sloan management review*, 38(3):93.

Lee, H. L., Padmanabhan, V., and Whang, S. (1997b). Information distortion in a supply chain: The bullwhip effect. *Management science*, 43(4):546–558.

Naudet, Y., Latour, T., Guedria, W., and Chen, D. (2010). Towards a systemic formalisation of interoperability. *Computers in Industry*, 61(2):176–185.

Rosener, V., Naudet, Y., and Latour, T. (2005). A model proposal of the interoperability problem. In *EMOI-INTEROP*.

Security, M. (2015). Cybercrime will cost businesses $2 trillion by 2019. http://www.securitymagazine.com/articles/86352-cybercrime-will-cost-businesses-2-trillion-by-2019 accessed in July 2017.