Blockchain Design and Modelling

Nicolae Sfetcu

February 17, 2019

Sfetcu, Nicolae, " Blockchain Design and Modelling", SetThings (February 17, 2019), MultiMedia Publishing (ed.), URL = https://www.setthings.com/en/blockchain-design-and-modelling/

Email: nicolae@sfetcu.com

This is a partial translation of
Sfetcu, Nicolae, " Filosofie tehnologiei blockchain - Ontologii", SetThings (1 februarie 2019), MultiMedia Publishing (ed.), DOI: 10.13140/RG.2.2.25492.35204, ISBN 978-606-033-154-4, URL = https://www.setthings.com/ro/e-books/filosofia-tehnologiei-blockchain-ontologii/

Blockchain Design and Models

Blockchain design

Ontology engineering, (Smith 2004) along with semantic Web technologies, allow the semantic development and modeling of the operational flow required for blockchain design. The semantic Web, in accordance with W3C, "provides a common framework that allows data to be shared and reused across application, enterprise, and community boundaries" (W3C 2013) and can be seen as an integrator for various content, applications and information systems. Tim Berners-Lee had the first vision of data network power (Berners-Lee 2007) processed by machines: (Berners-Lee 2004)

> “I have a dream for the Web [in which computers] become capable of analyzing all the data on the Web – the content, links, and transactions between people and computers. A Semantic Web

> , which should make this possible, has yet to emerge, but when it does, the day-to-day mechanisms of trade, bureaucracy and our daily lives will be handled by machines talking to machines. The intelligent agents people have touted for ages will finally materialize." (Berners-Lee 2000)

Metadata and semantic Web technologies have allowed the application of ontologies for the provenance of knowledge. Computational ontology research can be useful at the economic level (including for companies), socially, and for other researchers, contributing to the development of specific applications. (Kim and Laskowski 2016)

Many researchers regard computational ontology as a kind of applied philosophy. (Tom Gruber 2008) In the paper "*Toward Principles for the Design of Ontologies Used for Knowledge Sharing*," Tom Gruber delivers a deliberate definition of ontology as a technical term in the field of informatics. (Thomas Gruber 1994) Gruber introduced the term as a specification of conceptualization:

> "An ontology is a description (like a formal specification of a program) of the concepts and relationships that can exist for an agent or a community of agents. This definition is consistent with the usage of ontology as set-of-concept-definitions, but more general. And it is certainly a different sense of the word than its use in philosophy." (Tom Gruber 1992)

To distance ontologies from taxonomies, Gruber said: (Tom Gruber 1993)

> "Ontologies are often equated with taxonomic hierarchies of classes, but class definitions, and the subsumption relation, but ontologies need not be limited to these forms. Ontologies are also not limited to conservative definitions, that is, definitions in the traditional logic sense that only introduce terminology and do not add any knowledge about the world (Enderton, 1972) . To specify a conceptualization one needs to state axioms that do constrain the possible interpretations for the defined terms." (Tom Gruber 1993)

Feilmayr and Wöß have refined this definition: "An ontology is a formal, explicit specification of a shared conceptualization that is characterized by high semantic expressiveness required for increased complexity." (Feilmayr and Wöß 2016)

One of the most elaborated ontologies in this regard is the ontology of traceability (Kim, Fox, and Gruninger 1995) which helped to develop the TOVE ontologies for enterprise modeling (Fox and Grüninger 1998) considered as the main source for blockchain design.

Blockchain design is based on the fundamental principles of the Internet architecture: survival (Internet communications must continue despite network or gateway loss), variety of service types (multiple types of communications services), variety of networks (multiple types of networks), distributed resource management, profitability, ease of hosting, and responsibility in resource use. (Hardjono, Lipton, and Pentland 2018)

Blockchain models

The most widely used blockchain modelling system, by abstract representation, description and definition of structure, processes, information and resources, is the enterprises modelling. (Leondes and Jackson 1992) Enterprise modelling uses domain ontologies by model representation languages. (Vernadat 1997)

Based on component-based design, blockchain ontology decomposes blocks into functional or logical individual components, and identifies the possibilities, assisting in designing, implementing, and measuring the performance of different block architectures. (Tasca and Tessone 2017) According to Paolo Tasca, the methodological approach is basically composed of the following steps:

1. Comparative study of different blocks: vocabulary and term analysis to solve ambiguities and disagreements
2. Definition of the framework: identification and classification of components, defining a hierarchical ontology

3. Categorization of levels: Different aspects are introduced and compared for components from the lowest level of the hierarchical structure.

Like any ICT technology, a blockchain is driven by the fundamental principles of data decentralization, transparency, security and confidentiality. (Aste, Tasca, and Matteo 2017) Other fundamental features of blockchain include data automation and data storage capability.

According to Fox and Gruninger, from a design perspective, a business model should provide the language used to explicitly define an enterprise. (Fox and Grüninger 1998) From the perspective of operations, the enterprise modelling must be able to represent what is planned and what has happened, and provide the information and knowledge needed to support operations. (Fox and Grüninger 1998) Functions are modeled through a structured representation (FIPS PUBS 1993) a graphical representation in a field defined to identify information needs, identify opportunities and determine costs. (Department Of Defense (DOD) Records Management (RM) 1995) Other perspectives may be behavioral, organizational, or informational. (Koskinen 2000)

An appropriate blockchain functional modelling focuses on the process, using four symbols for this purpose:

- Process: Illustrates the transformation from input to output.
- Storage: Collecting data or other material.
- Flow: Moves data or materials into the process.
- External entity: External to the modelling system but interacting with it.

A process can be represented as a network of these symbols. In Dynamic Enterprise Modeling (DEMO), for example, a decomposition is done in the control model, function model, process model, and organizational model.

Data modelling uses the application of formal descriptions in a database. (Whitten, Bentley, and Dittman 2004) The data model will consist of entities, attributes, relationships, integrity rules and object definitions, being used to design the interface or the database.

Bibliography

Aste, Tomaso, Paolo Tasca, and Tiziana di Matteo. 2017. "Blockchain Technologies: The Foreseeable Impact on Society and Industry." *Computer* 50: 18–28. https://doi.org/10.1109/MC.2017.3571064.

Berners-Lee, Tim. 2000. *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web*. HarperCollins.

———. 2004. "Semantic Web." ResearchGate. 2004. https://www.researchgate.net/publication/307845029_Tim_Berners-Lee's_Semantic_Web.

———. 2007. "Q&A with Tim Berners-Lee - Bloomberg." 2007. https://www.bloomberg.com/news/articles/2007-04-09/q-and-a-with-tim-berners-leebusinessweek-business-news-stock-market-and-financial-advice.

Department Of Defense (DOD) Records Management (RM). 1995. "Reader's Guide to IDEF0 Function Models." https://www.archives.gov/files/era/pdf/rmsc-19951006-dod-rm-function-and-information-models.pdf.

Feilmayr, Christina, and Wolfram Wöß. 2016. "An Analysis of Ontologies and Their Success Factors for Application to Business." *Data & Knowledge Engineering* 101: 1–23. https://doi.org/10.1016/j.datak.2015.11.003.

FIPS PUBS. 1993. "FIPS Publication 183 Released of IDEFØ December 1993 by the Computer Systems Laboratory of the National Institute of Standards and Technology (NIST)." http://www.idef.com/wp-content/uploads/2016/02/idef0.pdf.

Fox, Mark Stephen, and Michael Grüninger. 1998. "Enterprise Modeling." ResearchGate. 1998. https://www.researchgate.net/publication/220604924_Enterprise_Modeling.

Gruber, Thomas. 1994. "Toward Principles for the Design of Ontologies Used for Knowledge Sharing." ResearchGate. 1994. https://www.researchgate.net/publication/2626138_Toward_Principles_for_the_Design_of_Ontologies_Used_for_Knowledge_Sharing.

Gruber, Tom. 1992. "What Is an Ontology?" 1992. http://www-ksl.stanford.edu/kst/what-is-an-ontology.html.

———. 1993. "A Translation Approach to Portable Ontology Specifications." 1993. http://tomgruber.org/writing/ontolingua-kaj-1993.htm.

———. 2008. "Ontology." 2008. http://tomgruber.org/writing/ontology-definition-2007.htm.

Hardjono, Thomas, Alexander Lipton, and Alex Pentland. 2018. "Towards a Design Philosophy for Interoperable Blockchain Systems." ResearchGate. 2018. https://www.researchgate.net/publication/325168344_Towards_a_Design_Philosophy_for_Interoperable_Blockchain_Systems.

Kim, Henry M., Mark S. Fox, and Michael Gruninger. 1995. "An Ontology of Quality for Enterprise Modelling." In , 105. IEEE Computer Society. http://dl.acm.org/citation.cfm?id=832309.837247.

Kim, Henry M., and Marek Laskowski. 2016. "Towards an Ontology-Driven Blockchain Design for Supply Chain Provenance." *ArXiv:1610.02922 [Cs]*. http://arxiv.org/abs/1610.02922.

Leondes, Cornelius T., and Richard Henry Frymuth Jackson. 1992. *Manufacturing and Automation Systems: Techniques and Technologies*. Academic Press.

Smith, Barry. 2004. "Beyond Concepts: Ontology as Reality Representation." In *Formal Ontology in Information Systems (FOIS)*, edited by Achille C. Varzi and Laure Vieu, 1–12.

Tasca, Paolo, and Claudio J. Tessone. 2017. "Taxonomy of Blockchain Technologies. Principles of Identification and Classification." *ArXiv:1708.04872 [Cs]*. http://arxiv.org/abs/1708.04872.

Vernadat, F. B. 1997. "Enterprise Modelling Languages." In *Enterprise Engineering and Integration: Building International Consensus Proceedings of ICEIMT '97, International Conference on Enterprise Integration and Modeling Technology, Torino, Italy, October 28–30, 1997*, edited by Kurt Kosanke and James G. Nell, 212–24. Research Reports Esprit. Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-60889-6_24.

W3C, W3C. 2013. "W3C Semantic Web Activity Homepage." 2013. https://www.w3.org/2001/sw/.

Whitten, Jeffrey L., Lonnie D. Bentley, and Kevin C. Dittman. 2004. *Systems Analysis and Design Methods*. McGraw-Hill Irwin.