Conception et modèles de blockchain - Bitcoin

Nicolae Sfetcu

04.06.2019

Sfetcu, Nicolae, « Conception et modèles de blockchain - Bitcoin », SetThings (4 juin 2019), URL = https://www.telework.ro/fr/conception-et-modeles-de-blockchain-bitcoin/

Email: nicolae@sfetcu.com

Une traduction partielle de :
Sfetcu, Nicolae, « Filosofia tehnologiei blockchain – Ontologii », SetThings (01.02.2019), MultiMedia Publishing (ed.), DOI: 10.13140/RG.2.2.25492.35204, ISBN 978-606-033-154-4, URL = https://www.telework.ro/ro/e-books/filosofia-tehnologiei-blockchain-ontologii/

Conception

L'ingénierie ontologique, (Smith 2004) associé aux technologies du Web sémantique, permet la modélisation sémantique et le développement du flux opérationnel requis pour la conception de la technologie blockchain (TB). Le Web sémantique, selon W3C, « fournit un cadre commun qui permet le partage et la réutilisation des données dans les applications d'entreprise, des entreprises et de la communauté, » (W3C 2013) et peut être considéré comme un intégrateur des divers contenus, applications et systèmes d'information. Tim Berners-Lee a été le premier qui a eu une vision de la puissance des réseaux de données (Berners-Lee 2007) traitées par les machines : (Berners-Lee 2004)

> « J'ai un rêve pour le Web capable d'analyser toutes les données sur le Web - le contenu, les liens et les transactions entre des personnes et des ordinateurs. Un « Web sémantique » qui rend cela possible va bientôt émerger, mais quand cela se produira, le commerce quotidien, la

> bureaucratie et la vie quotidienne seront traités par des machines qui parlent à des machines. Les « agents intelligents » que les gens ont recherchés au fil des siècles se concrétiseront finalement. » (Berners-Lee 2000)

Les métadonnées et les technologies du Web sémantique ont permis l'application d'ontologies pour obtenir des connaissances. La recherche en ontologie computationnelle peut être utile au niveau économique (y compris pour les entreprises), socialement et pour d'autres chercheurs, en contribuant au développement des applications spécifiques. (Kim and Laskowski 2016)

Beaucoup de chercheurs considèrent l'ontologie informatique comme une sorte de philosophie appliquée. (Tom Gruber 2008) Dans le document « *Sur les principes de conception des ontologies utilisées pour le partage de connaissances* », Tom Gruber propose une définition délibérée de l'ontologie en tant que terme technique dans le domaine de l'informatique. (Thomas Gruber 1994) Gruber a introduit le terme comme spécification de la conceptualisation :

> « Une ontologie est une description (en tant que spécification formelle d'un programme) des concepts et des relations pouvant exister formellement pour un agent ou une communauté d'agents. Cette définition est compatible avec l'utilisation de l'ontologie en tant qu'ensemble de définitions conceptuelles, mais plus générale. Et c'est un sens différent du mot que son utilisation en philosophie. » (Tom Gruber 1992)

En tentant de distancer les ontologies taxonomiques, Gruber a déclaré : (Tom Gruber 1993)

> « Les ontologies sont souvent assimilées aux hiérarchies taxonomiques de la classe, des définitions de classe et des relations de subsomption, mais les ontologies ne doivent pas être limitées à ces formes. Les ontologies ne se limitent pas non plus aux définitions conservatrices, c'est-à-dire aux définitions au sens logique traditionnel, qui n'introduisent que la terminologie et n'apportent aucune connaissance du monde. (Enderton 2001) Pour spécifier une conceptualisation, il est nécessaire de spécifier des axiomes empêchant toute interprétation possible des termes définis. » (Tom Gruber 1993)

Feilmayr et Wöß ont raffiné cette définition : « Une ontologie est une spécification formelle et explicite d'une conceptualisation commune, caractérisée par la forte expressivité sémantique requise pour une complexité accrue ». (Feilmayr and Wöß 2016)

L’une des ontologies les plus élaborées à cet égard est l’ontologie de la traçabilité, (Kim, Fox, and Gruninger 1995) qui a permis de développer les ontologies TOVE pour la modélisation d’entreprise, (Fox and Grüninger 1998) considérées comme la principale source de conception de la blockchain.

La conception de la blockchain est basée sur les principes fondamentaux de l'architecture Internet : la survie (les communications Internet doivent continuer malgré la perte du réseau ou de la passerelle), la variété des types de services (plusieurs types de services de communication), la variété des réseaux (plusieurs types de réseaux), la gestion distribuée des ressources, la rentabilité, la facilité d’attachement aux hôtes et la responsabilité dans l’utilisation des ressources. (Hardjono, Lipton, and Pentland 2018)

Modèles

Le système de modélisation blockchain le plus utilisé, par la représentation abstraite, la description et la définition de la structure, des processus, des informations et des ressources, est la modélisation des entreprises. (Leondes and Jackson 1992) La modélisation d'entreprise utilise des ontologies de domaine utilisant des langages de représentation du modèle. (Vernadat 1997)

Sur la base d'une conception à base de composants, l'ontologie blockchain décompose les blocs en composants individuels fonctionnels ou logiques et identifie les possibilités, en aidant à la conception, la mise en œuvre et la mesure des performances des différentes architectures de blocs. (Tasca and Tessone 2017) Selon Paolo Tasca, l'approche méthodologique comprend essentiellement les étapes suivantes :

1. Etude comparative des différents blocs : analyse de vocabulaire et termes permettant de résoudre des ambiguïtés et des désaccords

2. Définition du cadre : identification et classification des composants, définition d'une ontologie hiérarchique
3. Catégorisation des niveaux : différents aspects sont introduits et comparés pour les composants du niveau le plus bas de la structure hiérarchique.

Comme toute technologie informatique, une blockchain repose sur les principes fondamentaux de la décentralisation des données, de la transparence, de la sécurité et de la confidentialité. (Aste, Tasca, and Matteo 2017) Parmi les autres caractéristiques fondamentales de la blockchain, on peut citer l'automatisation et le stockage des données.

Selon Fox et Gruninger, d'un point de vue de la conception, un modèle d'entreprise devrait fournir le langage utilisé pour définir explicitement une entreprise. Du point de vue des opérations, le modèle d'entreprise doit pouvoir représenter ce qui est planifié et ce qui s'est passé et fournir les informations et les connaissances nécessaires au soutien des opérations. (Fox and Grüninger 1998) Les fonctions sont modélisées par une représentation structurée, une représentation graphique dans un champ défini pour identifier les besoins en informations, identifier les opportunités et déterminer les coûts. (Department Of Defense (DOD) Records Management (RM) 1995) D'autres perspectives peuvent être comportementales, organisationnelles ou informationnelles. (Koskinen 2000)

Une modélisation fonctionnelle appropriée de la TB est axée sur le processus et utilise quatre symboles à cette fin :

- Processus : Illustre la transformation de l'entrée à la sortie.
- Stockage : Collecte des données ou autre matériel.
- Flux : Déplace des données ou des matériaux dans le processus.
- Entité externe : Externe au système de modélisation, mais en interaction avec celui-ci.

Un processus peut être représenté comme un réseau de ces symboles. Dans DEMO (Dynamic Enterprise Modeling), par exemple, une décomposition est effectuée dans le modèle de contrôle, le modèle des fonctions, le modèle de processus et le modèle organisationnel.

La modélisation des données utilise l'application des descriptions formelles dans une base de données. (Whitten, Bentley, and Dittman 2004) Le modèle des données consistera en entités, attributs, relations, règles d'intégrité et définitions d'objet, utilisés pour concevoir l'interface ou la base de données.

Bitcoin

Bitcoin est le principal système de paiement pair-à-pair et cryptomonnaie qui utilise la technologie de la blockchain. Les fonctionnalités du réseau Bitcoin sont : (Calvery 2013)

- Il n'y a pas de serveur central, le réseau Bitcoin est pair-à-pair.
- Il n'y a pas de référentiel central, le registre Bitcoin est distribué.
- Le registre est public, tout le monde peut le stocker sur l'ordinateur.
- Il n'y a pas d'administrateur, le registre est géré par un réseau de mineurs ayant les mêmes privilèges.
- N'importe qui peut devenir mineur.
- Les ajouts au registre sont maintenus par voie de concurrence. Jusqu'à ce qu'un nouveau bloc soit ajouté au registre, on ne sait pas quel mineur créera le bloc.
- L’émission de bitcoins est décentralisée. Cette cryptomonnaie sont émises en guise de récompense pour la création d'un nouveau bloc.
- Tout le monde peut créer une nouvelle adresse bitcoin (une correspondance bitcoin d'un compte bancaire) sans approbation préalable.

- Tout le monde peut envoyer une transaction sur le réseau sans approbation préalable, le réseau ne fait que confirmer que la transaction est légitime.

Les chercheurs ont mis en évidence une « tendance à la centralisation » : d'une part, les mineurs de Bitcoin rejoignent de grandes bases minières afin de minimiser la variation de leurs revenus. (Böhme et al. 2015, 215–22) D'autre part, une « aristocratie » Bitcoin a été formée à la suite de l'architecture du code ; les membres de cette aristocratie sont ceux qui sont entrés tôt dans le jeu Bitcoin.

Dans *La vie sociale de Bitcoin*, Nigel Dodd affirme que l'essence de l'idéologie de Bitcoin est de retirer l'argent du contrôle social, y compris du gouvernement, il y a même une Déclaration d'indépendance Bitcoin. La déclaration inclut un message du crypto-anarchisme avec les mots : « Bitcoin est intrinsèquement anti-institution, antisystème et anti-état. Bitcoin sape les gouvernements et perturbe les institutions parce que le bitcoin est fondamentalement humanitaire ». (von Hayek 1976)

David Golumbia déclare que les idées qui influencent les partisans du bitcoin proviennent des mouvements extrémistes de droite et de leur rhétorique anti-banque centrale, ou plus récemment du libertarisme de Ron Paul et Tea Party. (The Economist 2018)

Kroll et al. soutiennent que l'écologie de Bitcoin aura besoin de structures de gouvernance pour survivre, (Kroll, Davey, and Felten 2013) montrant déjà des signes de structures de gouvernance émergentes. Ces modes de gouvernement peuvent être fondés sur le consensus et, si les dirigeants s’y opposent, la communauté peut choisir une autre voie. Au-delà de cela, les développements récents ont montré qu’un seul bassin minier pouvait tellement contribuer aux processus de calcul de Bitcoin, qu’il pouvait contrôler efficacement l’ensemble du système, mettant ainsi fin à sa structure décentralisée. (Kostakis and Giotitsas 2014)

Bauwens et Kostakis soutiennent que Bitcoin n'est pas un projet communautaire, mais une pièce représentant un nouveau type de capitalisme - un capitalisme « distribué », (Kostakis, Bauwens, and Niaros 2015) fondé sur l'idéologie politique libérale prônant l'élimination des états pour la souveraineté individuelle. En pratique, ce qui est réalisé est un capital concentré et une gouvernance centralisée.

Vasilis Kostakis et Chris Giotitsas considèrent également que Bitcoin est un exemple d'un type dérivé du « capitalisme distribué » (Kostakis and Giotitsas 2014) bien qu'il faille plutôt le considérer comme une innovation technologique.

Bibliographie

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.

Böhme, Rainer, Christin Nicolas, Edelman Benjamin, and Tyler Moore. 2015. "Bitcoin: Economics, Technology, and Governance." https://pubs.aeaweb.org/doi/pdfplus/10.1257/jep.29.2.213.

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.

Enderton, Herbert. 2001. "A Mathematical Introduction to Logic - 2nd Edition." 2001. https://www.elsevier.com/books/a-mathematical-introduction-to-logic/enderton/978-0-08-049646-7.

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.

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.
Hayek, Friedrich von. 1976. “Denationalisation of Money: The Argument Refined.” https://nakamotoinstitute.org/static/docs/denationalisation.pdf.
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.
Koskinen, Minna. 2000. “Process Perspectives. In: Metamodeling and Method Engineering.” http://users.jyu.fi/~jpt/ME2000/Me14/sld004.htm.
Kostakis, Vasilis, Michel Bauwens, and Vasilis Niaros. 2015. “Urban Reconfiguration after the Emergence of Peer-to-Peer Infrastructure: Four Future Scenarios with an Impact on Smart Cities.” In *Smart Cities as Democratic Ecologies*, edited by Daniel Araya, 116–24. London: Palgrave Macmillan UK. https://doi.org/10.1057/9781137377203_8.
Kostakis, Vasilis, and Chris Giotitsas. 2014. “The (A)Political Economy of Bitcoin.” ResearchGate. 2014. https://www.researchgate.net/publication/287241993_The_APolitical_Economy_of_Bitcoin.
Kroll, Joshua A., Ian C. Davey, and Edward W. Felten. 2013. “The Economics of Bitcoin Mining , or Bitcoin in the Presence of Adversaries.” In .
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.
The Economist. 2018. “Bitcoin and Other Cryptocurrencies Are Useless.” *The Economist*, 2018. https://www.economist.com/leaders/2018/08/30/bitcoin-and-other-cryptocurrencies-are-useless.
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.
Whitten, Jeffrey L., Lonnie D. Bentley, and Kevin C. Dittman. 2004. *Systems Analysis and Design Methods*. McGraw-Hill Irwin.