LEDGER
ledgerjournal.org

ISSN 2379-5980 (online)
Associated article DOI
10.5915/LEDGER.2019.140

A Taxonomy of Blockchain Technologies: Principles of Identification and Classification: Open Review

Authors: Paolo Tasca,[*][†] Claudio J. Tessone[‡]

Reviewers: Reviewer A, Reviewer B

Abstract. The final version of the paper "A Taxonomy of Blockchain Technologies: Principles of Identification and Classification" can be found in Ledger Vol. 4 (2019) 1-39, DOI 10.5915/LEDGER.2019.140. There were two reviewers involved in the review process, neither of whom have requested to waive their anonymity at present, and are thus listed as A and B. After initial review by Reviewers A and B (1A), it was determined that the submission required revisions. The author responded to their feedback (1B) and revised the manuscript. The Editors reviewed these changes and accepted the submission with minor revisions, thus completing the peer-review process. Author responses in 1B are bulleted and indented for clarity.

1A. Review

Reviewer A:

This paper provides a survey of blockchain and cryptocurrency projects and approaches, and offers an "ontology" to provide a glossary and comparative list of major approaches and technical challenges.

Overall I found this paper to be fairly superficial as a survey, and with many missing references to existing academic work with similar scope. The main constructive suggestions are to focus on critical analysis rather than taking the claims of each project at face value, and to do a more thorough job of citing existing academic work.

More detailed comments:

- 1.1 Gives background on blockchains, but not enough of a hint towards what needs to be addressed by the paper.

"the inability to efficiently share data," Sharing data efficiently seems like not a technical

[*] 3ELK15Knpz3bAB4t4VquvrW8gzi1oHMwXv

[†] P. Tasca (p.tasca@ucl.ac.uk) is founder and Executive Director of the Centre for Blockchain Technologies at the University College London, UK.

[‡] C. J. Tessone (claudio.tessone@business.uzh.ch) is Assistant Professor of Network Science at the University of Zurich and co-founder of the UZH Blockchain Centre.

problem, the internet has made information sharing very cheap for years. However, some new explanations that blockchain might address include the difficulty doing so securely, complicated regulations.

“More broadly, [blockchain] is a revolutionary method “
Blockchain is not given a definition here. Furthermore, blockchains are arguably a relabelling of existing well-studied techniques in security, distributed computing, and applied cryptography. This includes BFT protocols, the use of hash-based authenticated data structures, digital signatures and threshold cryptography.

- “p2. Currently there are thousands of blockchain projects worldwide under development, some of them” Run on sentence
- “An heterogeneous development” An -> A

The point seems to be that the fact there are many varied proposes and techniques is a “problem”, and therefore the solution is “standardised structures.” The premise that this heterogeneity is a problem could use more support.

“The aim of this study is to highlight the need for standard technical reference models”
This is a good statement to dig into and improve. The aim of the study should be falsifiable, i.e. to either find evidence either in support of this claim (e.g., to show that there must be standard reference models) or to show th

What is a standard technical reference model? Suppose we reframe the question: should a standard technical model be pursued explicitly, via standards bodies (this is then an call to action)? Or do standards emerge naturally as the market matures (in which case perhaps nothing new should be done, we should just wait….).

In 1.3, the focus of the study changes: “this study aims at proposing a rich blockchain Ontology” but it is not clear how providing an ontology can support or not support the question of need for standards.

- “Comparative study of different blockchains”

A comparative study would be better if it identified

Bonneau et al. http://www.jbonneau.com/doc/BMCNKF15-IEEESP-bitcoin.pdf is a missing citation, since it is a broad survey of cryptocurrency technology. It is also introduced several decoupled layers through which we can understand changed architectures, e.g., consensus layer, application layer, network layer. Could you compare this breakdown of layers to Bonneau et al.?

In general it is difficult to evaluate whether an ontology is *good* or not. I can offer some examples of things that may be missing, but as it is a moving target, it isn’t clear if including everything is what will make an ontology better. Alternative ontologies could choose different organizations, and I’m not sure how we’d identify which is better.

Figure 3. Doesn’t convey much information. I’m seen this common image before, which

ISSN 2379-5980 (online)
Associated article DOI
10.5915/LEDGER.2019.140

purports to offer a distinction between “decentralized” and “distributed,” but this actually has no meaningful distinction (and the text doesn’t mention this either).

Section 4.2 outlines the world of fault tolerant distributed systems, roughly from the point of view of a blockchain enthusiast who has not read any of the academic literature on fault tolerant distributed systems.

“Synereo is an example of blockchain using the an asynchronous communication protocol.”

- “Finality” This is commonly misunderstood.
All blockchains provide finality. More specifically, as long as the underlying assumptions are met, then there is a number of blocks to wait for such that finality is guaranteed except with negligible probability. “6 blocks” comes from nowhere except blog posts, so shouldn’t be taken seriously. But research analysis (see Bitcoin Backbone by Kiayias et al., and https://eprint.iacr.org/2016/555.pdf by Gervais et al., and more) provide more concrete analysis.
Even the “deterministic” protocols do not converge with certainty, since there is a small chance of a failure in hash collisions etc.

- “This blockchain ontology can be of practical importance in many cases.” The value of the ontology is suggested in 1.4, with 6 possible benefits. However, these are all speculative. It appears just as possible to me that the ontology will not succeed in having any of these effects. The paper would be improved if there were some evaluation applied to the artefact of the ontology itself. The null hypothesis (not to be too cynical!) is that the construction of an ontology was not productive.

Many of the concepts are superficial, essentially borrowed from popular media without much more depth.

“Security and immutability” - Many examples are now available where blockchains have changed, such as the Ethereum fork. A very good article on this topic is by Angela Walch https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2940335

There are several other surveys with similar scope as this. One is "Bitter to Better", FC 2012. A source of information to draw from would include this collection: https://cdecker.github.io/btcresearch/

Reviewer B:

1) Issue: There are numerous significant issues in the clarity of writing that need to be addressed before publication. These issues are more significant than “typos” or small grammatical errors, and they increase the difficulty of comprehension of the author.
• Recommendation: I think the fundamental clarity of the writing would benefit greatly from the use of a professional copy editor.

2) Issue: The methodology of this article is rather sound, but it is also premature. Developing

ISSN 2379-5980 (online)
Associated article DOI
10.5915/LEDGER.2019.140

a useful taxonomy in this area would be extremely helpful, but developing an ontology is early as new blockchains are emerging regularly. Protocols are still being developed through innovative practices regularly, and by creating an ontology, it could have a negative effect on the development of the technology.
• Recommendation: Through the same study focus on taxonomy, as opposed to ontology. Developing the vocabulary of the field into a coherent set of constructs and labels would be extremely useful at this juncture to moving the field forward.

3) Issue: In Section 2.1 you have an inconsistency that is important, and I'm not sure which way you want to stake your article. You state: "security and privacy, " then the sentence abruptly ends. But in the sections immediately below, you have a section entitled "security and immutability."
• Recommendation: I believe that security is quite a bit different from immutability deserving it's own section in a thorough ontological approach. But to that point, this is your article, and I respect your decisions as the author. Recommended Path: complete the introductory sentence to properly convey your thoughts, while aligning the section below. If you choose not to separate the two, it would be helpful to know why.

4) Issue: In section 2.2, you attempt to categorize blockchains by function. No categorization will make everyone happy. My question is where does digital identity fall? I see it in table 2, but am not sure how I would put it into a category. The visualizations as you proceed seem to be more helpful with regard to the dimensions. You really may consider that the bigger tables get moved to an appendix at the end, as they don't add as much value.
• Recommendation: Include examples of operationalizations of the categories in table 1. Add the next column, many readers won't know each coin you mention, so they don't actually know what is represented in that row.
• Table 1 as it stands is very cumbersome, because you explain each coin the way that you do. I would consider including a category definition instead of a description of the technology. If you feel strongly about including a description of each coin, do a comprehensive list and attach it as an appendix.

5) Now that I have read the entire paper a couple of times, I'm more convinced of the usefulness of the ontological approach that you have taken. I think it is very thorough. If you choose to persist in this approach, I don't know that you should not get more specific and write an actual book. This is already a very long journal article. In the event that you don't follow recommendation 2.a., I believe it is in your best interest to reconceptualize the front end of the paper. Your argument for an ontology could be based upon the need to know what we already know so we can move forward and look at gaps, rather than looking at what is out there so that we can standardize at this point.

6) Sections 4.2 need to be beefed up. For instance, #2 Proof of Stake. I think that a reader should find enough information that it can actually understand how proof of stake works. Quickly searching github, I find better explanations with different terms (uniformity of terminology is difficult).

7) Section 5.5 Limits to Scalability: Query whether it is worth discussing particular chains approaches to tackling scaling issues in the future? Should you consider the issues are

ISSN 2379-5980 (online)
Associated article DOI
10.5915/LEDGER.2019.140

segwit2x, transformation to proof of stake and sharding at eth, etc.

8) I was particularly impressed with your work through the fee structures in 11.2.2. Thank you for your work.

9) In your conclusion, you argue that software architects, companies, and regulators want standardization. Yes, standardization is important, at some point in time. Why do you think it is important today? We haven’t solved scalability issues yet to the point that we are implementing solutions in large scalable commercial settings.

I would argue from the perspective of a Technology Innovation Management scholar that we need to continue searching for the protocols necessary to be able to scale based upon transactions, persons, and nodes. As you begin to argue for standardization and the widespread adoption of blockchain technologies, you assume that it is a good thing. Yet, an alternative answer is that the technology hasn’t matured to the point that it is ready for widespread adoption. Most timelines that I have seen or discussed really look at 2019-2022 as the time frame for the beginning of this adoption. Also, is this article designed to support the adoption or is it designed to describe the properties & relationships regarding the blockchains.

I think attention to performing the ontological study, as opposed to worrying about why you are performing the ontology may alleviate my concerns listed in comment 2 above.

1B. Authors’ Responses

Reviewer A:

This paper provides a survey of blockchain and cryptocurrency projects and approaches, and offers an "ontology" to provide a glossary and comparative list of major approaches and technical challenges.

Overall I found this paper to be fairly superficial as a survey, and with many missing references to existing academic work with similar scope. The main constructive suggestions are to focus on critical analysis rather than taking the claims of each project at face value, and to do a more thorough job of citing existing academic work.

More detailed comments:

- 1.1 Gives background on blockchains, but not enough of a hint towards what needs to be addressed by the paper.

  - Thank you for your comment.

“the inability to efficiently share data,” Sharing data efficiently seems like not a technical problem, the internet has made information sharing very cheap for years. However, some new

ISSN 2379-5980 (online)
Associated article DOI
10.5915/LEDGER.2019.140

explanations that blockchain might address include the difficulty doing so securely, complicated regulations.

- Thank you for your comment.

“More broadly, [blockchain] is a revolutionary method”
Blockchain is not given a definition here. Furthermore, blockchains are arguably a relabelling of existing well-studied techniques in security, distributed computing, and applied cryptography. This includes BFT protocols, the use of hash-based authenticated data structures, digital signatures and threshold cryptography.

- Thank you for your comment.

- “p2. Currently there are thousands of blockchain projects worldwide under development, some of them” Run on sentence

- Thank you for your grammatical advice.

- “An heterogeneous development” An -> A

- Thank you for your grammatical advice.

The point seems to be that the fact there are many varied proposes and techniques is a “problem”, and therefore the solution is “standardised structures.” The premise that this heterogeneity is a problem could use more support.

- Thank you for your comment.

“The aim of this study is to highlight the need for standard technical reference models”
This is a good statement to dig into and improve. The aim of the study should be falsifiable, i.e. to either find evidence either in support of this claim (e.g., to show that there must be standard reference models) or to show th

- Our study does not introduce a new model - elaborated out of a new theory - that must be falsifiable. Our study is a literature review which by definition does not have falsifiable criteria. Our claim that “we need standard reference models” is based on a priors according to which precedent taxonomies/ontologies of other technologies have been used in other domains for defining those technologies’ standards.

What is a standard technical reference model? Suppose we reframe the question: should a standard technical model be pursued explicitly, via standards bodies (this is then an call to action)? Or do standards emerge naturally as the market matures (in which case perhaps nothing new should be done, we should just wait….).

- Thank you for your comment. Standards can emerge either naturally because of

ISSN 2379-5980 (online)
Associated article DOI
10.5915/LEDGER.2019.140

market adoption (industry driven) or because imposed by institutes and organisations. The paper does not take any position with respect to the origin of the standards. We do not promote the emergence of standards driven by institutes for standardizations or by the market.

In 1.3, the focus of the study changes: "this study aims at proposing a rich blockchain Ontology" but it is not clear how providing an ontology can support or not support the question of need for standards.

- Please see response to comment at the bottom of page vi.

- "Comparative study of different blockchains" A comparative study would be better if it identified

- Thank you for your comment. We have adjusted the wording to "analysis across blockchains".

Bonneau et al. http://www.jbonneau.com/doc/BMCNKF15-IEEESP-bitcoin.pdf is a missing citation, since it is a broad survey of cryptocurrency technology. It is also introduced several decoupled layers through which we can understand changed architectures, e.g., consensus layer, application layer, network layer. Could you compare this breakdown of layers to Bonneau et al.?

- The authors manly focus on Bitcoin. Nevertheless, they provide a useful framework and identify main technical components: transactions (including scripts), the consensus protocol, and the communication network. Our work is more general and abstract from Bitcoin. We nevertheless cite the authors several times in our manuscript.

In general it is difficult to evaluate whether an ontology is *good* or not. I can offer some examples of things that may be missing, but as it is a moving target, it isn't clear if including everything is what will make an ontology better. Alternative ontologies could choose different organizations, and I'm not sure how we'd identify which is better.

- We fully agree with your comment. Taxonomies / ontologies are developed to serve different purposes. Therefore it is not possible and not advisable to elaborate a rank of good/bad taxonomies or ontologies. The problem is similar to the elaboration of geographic maps. Among different maps of the same area, which one is the best?

Figure 3. Doesn't convey much information. I'm seen this common image before, which purports to offer a distinction between "decentralized" and "distributed," but this actually has no meaningful distinction (and the text doesn't mention this either).

- Thank you for your comment. We know that the picture has been used in several other blockchain related documents, but we have used the picture for the seek of completeness. In our approach we have described every layout with an appropriate pictogram.

Section 4.2 outlines the world of fault tolerant distributed systems, roughly from the point of view of a blockchain enthusiast who has not read any of the academic literature on fault tolerant distributed systems.

- Thank you for your comment. Given the limitation of space in the article and the broad target audience, the language is kept general as we cannot deeply explains all the technical concepts. However, we have rewritten section 4.2 and addressed the reader to the literature in order to deeper analyise the concepts introduced in the Section.

“Synereo is an example of blockchain using the an asynchronous communication protocol.”

- “Finality” This is commonly misunderstood.
All blockchains provide finality. More specifically, as long as the underlying assumptions are met, then there is a number of blocks to wait for such that finality is guaranteed except with negligible probability. “6 blocks” comes from nowhere except blog posts, so shouldn’t be taken seriously. But research analysis (see Bitcoin Backbone by Kiayias et al., and https://eprint.iacr.org/2016/555.pdf by Gervais et al., and more) provide more concrete analysis.

- We are thankful to the referee for correctly pointing out our incorrect introduction of the term. Indeed, in the revised manuscript, we have corrected the concept of finality, while preserving the layouts, where the concept was correctly used.

Even the “deterministic” protocols do not converge with certainty, since there is a small chance of a failure in hash collisions etc.

- “This blockchain ontology can be of practical importance in many cases.” The value of the ontology is suggested in 1.4, with 6 possible benefits. However, these are all speculative. It appears just as possible to me that the ontology will not succeed in having any of these effects. The paper would be improved if there were some evaluation applied to the artefact of the ontology itself. The null hypothesis (not to be too cynical!) is that the construction of an ontology was not productive.

- We have rephrased all the article in terms of Taxonomy according to reviewer B’s suggestion. Our Taxonomy could be used by those that in the future would like to

ISSN 2379-5980 (online)
Associated article DOI
10.5915/LEDGER.2019.140

propose an Ontology when the development of the technology will be more mature. At the same time, our taxonomy can help everybody to think according to the same terms and logics. This is our contribution and as explained in our reply to comment 8, it cannot be falsifiable.

Many of the concepts are superficial, essentially borrowed from popular media without much more depth.

- We have taken this concept by the referee seriously, and we have corrected, where necessary, the terms throughout all the manuscript to avoid this wrong impression. The referee should acknowledge, however, that this is a review article, and going into details (or not using layman's language) is very difficult if the audience of the eventual paper is broad. Addressing such multidisciplinary target is difficult if one enters into a technical jargon. Our intention is the manuscript to serve as a gateway such that researchers and practitioners oversee the complexities involved in blockchain-based technologies and find the reference to the literature if they want to dig into some specific concept.

“Security and immutability” - Many examples are now available where blockchains have changed, such as the Ethereum fork. A very good article on this topic is by Angela Walch https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2940335

- The referee is correct. We have now discussed in the same section the importance that the governing body - even if informal - has on the history recorded in the blockchains. A highly non-trivial discussion, which merits its own research line. We have further added the citation to the celebrated work by Barber et al. that was unrightfully neglected.

There are several other surveys with similar scope as this. One is "Bitter to Better", FC 2012. A source of information to draw from would include this collection: https://cdecker.github.io/btcresearch/

- Citation added: Bitter to Better — How to Make Bitcoin a Better Currency, International Conference on Financial Cryptography and Data Security FC 2012: Financial Cryptography and Data Security pp 399-414. Simon Barber, Xavier Boyen, Elaine Shi, Ersin Uzun.

ISSN 2379-5980 (online)
Associated article DOI
10.5915/LEDGER.2019.140

Reviewer B:

1) Issue: There are numerous significant issues in the clarity of writing that need to be addressed before publication. These issues are more significant than "typos" or small grammatical errors, and they increase the difficulty of comprehension of the author.
• Recommendation: I think the fundamental clarity of the writing would benefit greatly from the use of a professional copy editor.

- Thank you for the comment. We have improved the grammar along all the manuscript. We have improved the grammar and the fluency of the reading.

2) Issue: The methodology of this article is rather sound, but it is also premature. Developing a useful taxonomy in this area would be extremely helpful, but developing an ontology is early as new blockchains are emerging regularly. Protocols are still being developed through innovative practices regularly, and by creating an ontology, it could have a negative effect on the development of the technology.
• Recommendation: Through the same study focus on taxonomy, as opposed to ontology. Developing the vocabulary of the field into a coherent set of constructs and labels would be extremely useful at this juncture to moving the field forward.

- Thank you for your comments that we have considered very seriously. We indeed agree with your observation and - although keeping the same structure - we have changed all the article from "Ontology" to "Taxonomy". In introduction we added a definition of ontology and taxonomy and we specified that in the manuscript we focus on taxonomy.

3) Issue: In Section 2.1 you have an inconsistency that is important, and I'm not sure which way you want to stake your article. You state: "security and privacy, " then the sentence abruptly ends. But in the sections immediately below, you have a section entitled "security and immutability."
• Recommendation: I believe that security is quite a bit different from immutability deserving it's own section in a thorough ontological approach. But to that point, this is your article, and I respect your decisions as the author. Recommended Path: complete the introductory sentence to properly convey your thoughts, while aligning the section below. If you choose not to separate the two, it would be helpful to know why.

- Thank you to the referee for the comments. We have clarified better this part in the manuscript and split "security" from "immutability". However, we would like to inform the referee that the list of terms and concepts introduced in Section 2.1 is only propaedeutic to a general preliminary discussion about blockchain and It do not relates to the taxonomy that will be developed later in the manuscript.

4) Issue: In section 2.2, you attempt to categorize blockchains by function. No categorization

ISSN 2379-5980 (online)
Associated article DOI
10.5915/LEDGER.2019.140

will make everyone happy. My question is where does digital identity fall? I see it in table 2, but am not sure how I would put it into a category. The visualizations as you proceed seem to be more helpful with regard to the dimensions. You really may consider that the bigger tables get moved to an appendix at the end, as they don't add as much value.
- Recommendation: Include examples of operationalizations of the categories in table 1. Add the next column, many readers won't know each coin you mention, so they don't actually know what is represented in that row.
- Table 1 as it stands is very cumbersome, because you explain each coin the way that you do. I would consider including a category definition instead of a description of the technology. If you feel strongly about including a description of each coin, do a comprehensive list and attach it as an appendix.

- Digital identity is part of the component "Identity management". Actually a global property of all the subcomponents that compose it. In order to better clarify this point, we have rewritten the specific text. We have also reworked the Table 1 and put it in Appendix as the categorization was indeed a bit cumbersome and not useful to understand the taxonomy work. Table 1 *is* giant. We cannot see anything useful. We have replaced it and created a taxonomy Tree. We decided also to remove completely Section 2.2 as it was not properly linked to the logic behind the work on taxonomy conducted in the remaining part of the analysis.

5) Now that I have read the entire paper a couple of times, I'm more convinced of the usefulness of the ontological approach that you have taken. I think it is very thorough. If you choose to persist in this approach, I don't know that you should not get more specific and write an actual book. This is already a very long journal article. In the event that you don't follow recommendation 2.a., I believe it is in your best interest to reconceptualize the front end of the paper. Your argument for an ontology could be based upon the need to know what we already know so we can move forward and look at gaps, rather than looking at what is out there so that we can standardize at this point.

- In line with the requirements of the referee, we have rewritten that part of the manuscript.

6) Sections 4.2 need to be beefed up. For instance, #2 Proof of Stake. I think that a reader should find enough information that it can actually understand how proof of stake works. Quickly searching github, I find better explanations with different terms (uniformity of terminology is difficult).

- We have pervasively rewritten 4.2 according to the suggestions by the referee.

7) Section 5.5 Limits to Scalability: Query whether it is worth discussing particular chains approaches to tackling scaling issues in the future? Should you consider the issues are segwit2x, transformation to proof of stake and sharding at eth, etc.

ISSN 2379-5980 (online)
Associated article DOI
10.5915/LEDGER.2019.140

- In agreement with the referee requirement, we have modified the text and highlighted the fact that many of these systems' limitations to scalability may depend of specific implementations (now or in the future)

8) I was particularly impressed with your work through the fee structures in 11.2.2. Thank you for your work.

9) In your conclusion, you argue that software architects, companies, and regulators want standardization. Yes, standardization is important, at some point in time. Why do you think it is important today? We haven't solved scalability issues yet to the point that we are implementing solutions in large scalable commercial settings.

- We thank you the referee for the comment. Our work does not claim or conclude that we need a define set of blockchain standards now. With our work we simply shed light on the need for blockchain standards and present a literature review of the major blockchains in order to propose a taxonomy that could be preparatory for the current discussions about blockchain standards. We have explained in the Conclusions why we think that our work was important to be done now although we do not take any position whether standards should be developed now.

I would argue from the perspective of a Technology Innovation Management scholar that we need to continue searching for the protocols necessary to be able to scale based upon transactions, persons, and nodes. As you begin to argue for standardization and the widespread adoption of blockchain technologies, you assume that it is a good thing. Yet, an alternative answer is that the technology hasn't matured to the point that it is ready for widespread adoption. Most timelines that I have seen or discussed really look at 2019-2022 as the time frame for the beginning of this adoption. Also, is this article designed to support the adoption or is it designed to describe the properties & relationships regarding the blockchains.

I think attention to performing the ontological study, as opposed to worrying about why you are performing the ontology may alleviate my concerns listed in comment 2 above.

- Dear referee, we have solved this issue as we rephrase our study as a preliminary "Taxonomy" of blockchains as per your suggestion in comment 2. We are aware of the fact that blockchain is evolving over time and that our Taxonomy exercise is very preliminary although very useful.

Articles in this journal are licensed under a Creative Commons Attribution 4.0 License.

Ledger is published by the University Library System of the University of Pittsburgh as part of its D-Scribe Digital Publishing Program and is cosponsored by the University of Pittsburgh Press.

ISSN 2379-5980 (online)
Associated article DOI
10.5915/LEDGER.2019.140