Human-based Consensus for Trust Installation in Ontologies

Christoph Summerer [A,B] christoph.summerer@gmx.de
Emanuel Regnath [B] emanuel.regnath@tum.de
Hans Ehm [A] hans.ehm@infineon.com
Sebastian Steinhorst [B] sebastian.steinhorst@tum.de

***Abstract*—In this paper, we propose a novel protocol to represent the human factor on a blockchain environment. Our approach allows single or groups of humans to propose data in blocks which cannot be validated automatically but need human knowledge and collaboration to be validated. Only if human-based consensus on the correctness and trustworthiness of the data is reached, the new block is appended to the blockchain. This human approach significantly extends the possibilities of blockchain applications on data types apart from financial transaction data.**

***Index Terms*—Blockchain, Semantic Web, Ontologies, Trust**

I. Introduction

Blockchain technology is considered as a big "trust machine" [1] due to its immutability and traceability properties. While crypto-currencies such as Bitcoin [2] focus on storing transactions of financial assets in the blockchain, in general, this is also possible for other data types that can often not be validated automatically but require human thinking. This human factor not only influences the way of applying blockchain technologies for such content but also the way of reaching distributed consensus on it. For that reason, it is necessary to extend conventional blockchain and consensus processes to that human factor. One example for this is Semantic Web content, so-called ontologies, which represent linked data in the Web Ontology Language. Since there are currently only a few standards available, these ontologies are under constant development and there is no standardized way to install trust into them yet. The validation of those ontologies can only be done by human experts and there is currently no mechanism to integrate this into a blockchain architecture. As a result, it is not possible to use human validation of data and blockchain security together, which could lead to a chaotic and inconsistent Semantic Web development. To prevent this, we developed an approach that aligns the processes on a blockchain to this human factor in order to harmonize ontology creation across several domains and stakeholders.

A. Contributions

We propose the combination of blockchain technologies with human validation and confirmation of data on the example of ontology data, as illustrated in Figure 1. In particular, we enable

- the single and joint proposal-making of changes applied to an ontology,
- stake adjustment towards the size and impact of proposed changes in an ontology, and
- human validation and consensus-finding on changes in an ontology that eventually results in a final block representing the latest trusted single source of truth.

[A] Infineon Technologies AG, Germany
[B] Technical University of Munich, Germany

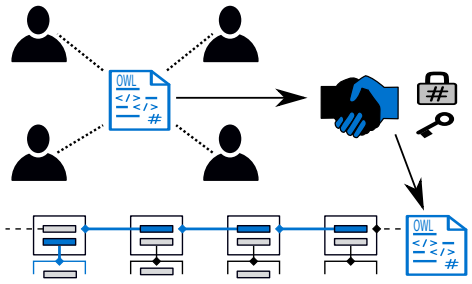

Figure 1: Concept of our human-based consensus approach.

II. Our Human-based Consensus Approach

We consider a blockchain $\mathbf{C}$ that stores ontology data in blocks $\mathcal{B}_i$ ordered over time. The length of $\mathbf{C}$ is n and i represents the index of block $\mathcal{B}_i$, following [2]. Before a new block is to the blockchain, we consider it as a block proposal $\mathcal{P}_i$. Each participant or even a group of participants in the private network can propose changes or improvements in the ontology by including the new version of the ontology into $\mathcal{P}_i$. Furthermore, we define a set of human validators V that validate $\mathcal{P}_i$ for correctness and reach distributed human-based consensus on it.

a) Consensus Algorithm We base our human-based consensus on Practical Byzantine Fault Tolerance (PBFT) [3] and extend it by a human voting mechanism. After validating $\mathcal{P}_i$, V can either agree or disagree with $\mathcal{P}_i$ by casting a vote. Should a majority of V consider the proposed changes in the ontology to be correct, distributed human-based consensus is reached and the proposed version of the ontology is integrated into $\mathcal{B}_i$ and appended to $\mathbf{C}$. $\mathcal{P}_n$ in $\mathbf{C}$ then represents and contains the latest accepted and trusted version of this ontology. This procedure is shown in Figure 2. In general, our human-based consensus can be applied for any kind of data that needs to be validated and confirmed by humans before it can be written into a blockchain.

b) Token System We propose a non-monetary token system $\mathbf{T}$, based on stake $\mathcal{S}$ and reward $\mathcal{R}$: $\mathbf{T} = \{\mathcal{S}, \mathcal{R}\}$. We distinguish between reward tokens for the proposer of $\mathcal{P}_i$, $\mathcal{R}_{P,i}$, and reward tokens for the validators in V, $\mathcal{R}_{V,i}$. For each proposal $\mathcal{P}_i$, a number of tokens that is adjusted to the size and impact of $\mathcal{P}_i$ has to be deposited as a stake $\mathcal{S}_i$. If $\mathcal{P}_i$ is rejected, $\mathcal{S}_i$ gets lost. By contrast, if $\mathcal{P}_i$ is accepted by a majority, the proposer gets rewarded by a multiple of the deposited stake $\mathcal{R}_{P,i} = 3 \cdot \mathcal{S}_i$ and also the validators get a reward $\mathcal{R}_{V,i} = 1 \cdot \mathcal{S}_i$. In the case of joint proposals, stake and reward are equally distributed among the involved peers. This token system allows only peers with a certain amount of tokens, gained by honest and active participation in the

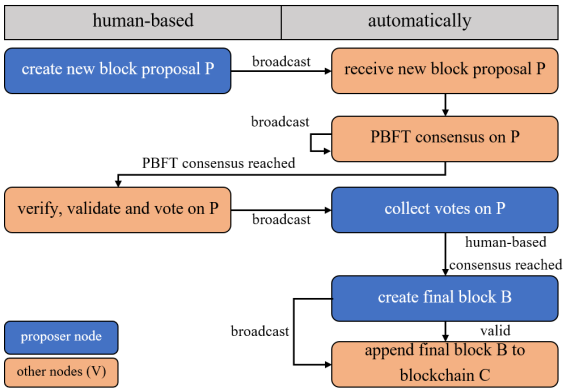

Figure 2: Human-based consensus approach.

network, to make new proposals and, by this, prevents the network from being flooded with meaningless requests.

c) Metrics To make the human-based decision process more transparent, we introduce metrics about the proposer and the proposal itself and include them directly in the block data. Thereby, users can understand who made which proposal $\mathcal{P}_i$ at which time and by how many other humans in V it was validated and considered to be correct and trustworthy.

d) Implementation We implemented a prototype of our approach using the Go programming language, which offers advantages in terms of speed, platform interoperability, multi-threading, safety and user-friendliness. We made use of `go-libp2p`, a modular network stack that allows a lot of blockchain-related features, and the Inter Planetary File System (IPFS), a distributed file system that allows to store and share data within a decentralized peer-to-peer network. The encrypted message flow in this private network is shown in Figure 2. The code is publicly available [4] for review and further research.

III. Related Work

Consensus as a prerequisite for trustable ontologies was recognized by [5] and [6] and later extended by [7]. The authors conclude that contradictory interpretations of ontologies are counterproductive for the installation of trust and propose a fuzzy voting model to agree on one state. However, none of those approaches is intended to be applied on a blockchain. [8] and [9] propose to apply blockchain technologies to implement the trust layer of the Semantic Web. However, there is no distributed consensus part in those approaches. The blockchain is more used as a distributed logbook rather than acting as a trust machine. [10] proposes to track the interactions of scientific publishers and contributors for academic publications on a blockchain. Nevertheless, also in that approach, no real distributed consensus is found. [11] proposes a consensus algorithm called Proof of Vote (POV) for permissioned consortium blockchains. It defines a fixed set of trusted roles that work together to create and vote on new blocks in the chain. In contrast to our approach, proposing new blocks is limited to certain roles. Furthermore, POV is not explicitly a human-based consensus method as the proposed roles could also be executed by non-human devices.

	Consensus	Blockchain	Joint proposals
[7]	✓	✗	✓
[8]	✗	✓	✗
[9]	✗	✓	✗
[10]	✗	✓	✗
[11]	(✓)	✓	✗
Our Work	✓	✓	✓

Table I: Comparison of our approach with related work.

IV. Evaluation and Discussion

As human behavior is hard to simulate and can vary from domain to domain, we decided to focus on an analytical comparison of our approach with others and added a short experimental validation to prove its practical functionality.

a) Analytical Comparison Table I compares our human-based consensus approach with other related approaches presented in Section III.

Our approach is the only one that combines human-based consensus with blockchain benefits and enables joint proposals. It allows to dynamically adjust the network of human experts by removing or adding peers during runtime. Since a non-monetary token system **T** is used, the overall costs are rather low, consisting of operating costs and costs for the invested working time of human experts. As our approach considers human-created ontology data, in comparison with financial transaction data it does not achieve a too high number of transactions. Furthermore, the network size is limited to a small number of experts. Since our approach is based on PBFT, its properties in terms of safety, liveness, fault-tolerance and transaction finality can be adopted. However, the scalability of our approach is limited by the message exchange, as proposals, votes and decisions have to be exchanged and processed in the entire decentralized network.

b) Experimental Validation We tested our implementation on the example of the Digital Reference [12], an ontology developed at H2020/ECSEL/productive4.0 [13] and currently being extended in the corresponding corporate support action SC³ [14]. This Digital Reference represents the semiconductor supply chain and supply chains containing semiconductors. The human validation of the Digital Reference requires not only a high number of messages being exchanged, but also more time compared with automatically validated financial transaction data. Our experiments have shown that, depending on network size and proposal type, the time between proposal-making and consensus-finding can vary between seconds and minutes or even hours and days. To sum up, our approach strongly depends on the hardly predictable behavior of the human experts in the network, which is why no fixed information on performance, transaction rate, latency etc. can be given.

V. Conclusion

Our proposed human-based consensus approach is, to the best of our knowledge, the only one combining human collaboration, human-based consensus-finding on ontologies and blockchain technologies at the same time. The implementation of our approach has shown that it can be practically applied.

REFERENCES

[1] "The trust machine," https://www.economist.com/leaders/2015/10/31/the-trust-machine, (Accessed on 07/08/2019).

[2] J. Garay, A. Kiayias, and N. Leonardos, "The bitcoin backbone protocol: Analysis and applications," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2015.

[3] M. Castro, B. Liskov *et al.*, "Practical byzantine fault tolerance," in *OSDI*, vol. 99, 1999.

[4] TUM-ESI, "Our Prototypical Implementation in Go," https://github.com/tum-esi/human-bc-consensus.

[5] M. Nagy and M. Vargas-Vera, "Reaching consensus over contradictory interpretation of semantic web data for ontology mapping," in *5th Int. Conf. on Intelligent Computer Communication and Processing*. IEEE, 2009.

[6] M. Nagy, M. Vargas-Vera, and E. Motta, "Managing conflicting beliefs with fuzzy trust on the semantic web," in *Mexican International Conference on Artificial Intelligence*. Springer, 2008.

[7] T. H. Duong, M. Q. Tran, and T. P. T. Nguyen, "Collaborative vietnamese wordnet building using consensus quality," *Vietnam Journal of Computer Science*, vol. 4, no. 2, 2017.

[8] B. Iancu and C. Sandu, "A cryptographic approach for implementing semantic web's trust layer," in *International Conference for Information Technology and Communications*. Springer, 2016.

[9] H.-G. Fill and F. Härer, "Knowledge blockchains: Applying blockchain technologies to enterprise modeling," 2018.

[10] M. R. Hoffman, L.-D. Ibáñez, H. Fryer, and E. Simperl, "Smart papers: Dynamic publications on the blockchain," in *European Semantic Web Conference*. Springer, 2018.

[11] K. Li *et al.*, "Proof of vote: A high-performance consensus protocol based on vote mechanism & consortium blockchain," in *19th Int. Conf. on High Performance Computing and Communications*. IEEE, 2017.

[12] Ehm, Hans and Dimitrakopoulos, George, "Digital Reference ontology," http://www.w3id.org/ecsel-dr/.

[13] "H2020, ecsel joint undertaking and national funding from 19 involved countries under grant-agreement no. gap-737459 – 999978918, productive4.0," https://productive40.eu/, (Accessed on 11/30/2020).

[14] "H2020, ecsel csa sc³, id: 101007312," https://cordis.europa.eu/project/id/101007312, (Accessed on 11/30/2020).