INTERNET POLICY REVIEW
Journal on internet regulation

Reputation
Volume 10 **Issue** 2

GLOSSARY ENTRY

OPEN ACCESS

PEER REVIEWED

Reputation

Primavera De Filippi *Harvard University* **Ori Shimony** *dOrg* ori@dorg.tech
Antonio Tenorio-Fornés *Complutense University of Madrid* antoniotenorio@ucm.es

DOI: https://doi.org/10.14763/2021.2.1547

Published: 19 April 2021
Received: 11 November 2020 **Accepted:** 2 December 2020

Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Citation: De Filippi, P. & Shimony, O. & Tenorio-Fornés, A. (2021). Reputation. *Internet Policy Review*, *10*(2). https://doi.org/10.14763/2021.2.1547

Keywords: Reputation, Blockchain, Identity

Abstract: Reputation in a blockchain-based system is a digital representation of an entity's standing or status in a specific domain.

This article belongs to the **Glossary of decentralised technosocial systems**, a special section of *Internet Policy Review*.

Definition

Reputation in a blockchain-based system is a digital representation of an entity's standing or status in a specific domain.

Origin and evolution of the term

A. Origin

Technologies such as the internet, or blockchain, enable large scale interactions among total strangers. Reputation systems (Resnick et al., 2000) appeared as a solution to facilitate these interactions when some level of trust was required, such as in online shopping in peer to peer marketplaces like eBay, or online production communities (Benkler, 2006). Yet, these systems generally relied on a centralised operator, in charge of managing user reputation.

There are several decentralised reputation systems (Hendrikx, 2015), most relying either on maintaining a personal list of trusted and untrusted nodes; aggregating such reputation information from other trusted nodes (with certain degree of transitivity such as in web-of-trust); or using Distributed Hash Tables to manage a global directory of semi-trusted nodes (Chawathe et al., 2003).

Blockchain technology introduces the possibility for a next generation of reputation systems that utilise persistent global state and immutable transaction histories. This allows for transparency and security guarantees that were unavailable in previous distributed systems. Furthermore, the openness and persistence of blockchains makes them a valuable tool to support shared data stores that can be leveraged by multiple services, thereby enhancing reputation portability and interoperability.

B. Evolution

Bitcoin (Nakamoro, 2009) relied on blockchain technology to create a distributed payment system operating on top of a peer-to-peer network. The operations of Bitcoin did not rely on trust or reputation. Instead, the influence of every network node is determined by the amount of resources engaged into the network: the

greater the amount of resources, the more influence one has in the network. Many of the other blockchain-based networks that followed suit relied on similar protocols, also based on a resource-driven model (i.e. the amount of hashing power in the case of Proof-of-Work or the amount of tokens holding in the case of Proof-of-Stake).

Early reputation systems have been implemented at the infrastructure layer, as trust-based alternatives to the **Proof-of-Work** or **Proof-of-Stake** consensus algorithm. For instance, delegated **Proof-of-Stake** (Larimer, 2014) allows for a more meritocratic system, based on merit or perceived trustworthiness. As a result, anyone holding a particular amount of reputation within a blockchain community will have influence in proportion to the amount of reputation they hold.

At the application layer, the introduction of "reputation" in the blockchain space was also an attempt to move away from the perception of blockchain technology as a purely trustless system, to enable the establishment of more sophisticated systems where some actors *can* be trusted. As argued by Hawlitschek and colleagues (Hawlitschek et al., 2018), the introduction of "reputation" is necessary for the establishment of trustless systems that operationally rely on trust. On the one hand, trustless systems such as Bitcoin are based on the assumption that no one *can* or *shall* be trusted. Hence, these systems are designed to entirely eliminate the need for trust, relying on cryptographic primitives and proofs in order to ensure that people behave according to the rules (Ali et al., 2016). On the other hand, there are many human-sensitive services (e.g., peer-to-peer marketplaces like Uber, Airbnb, or eBay) based on the assumption that some actors can be trusted to behave honestly. These systems rely on "reputation" in order to help users assess the trustworthiness of the other users interacting on these platforms. In order to provide these types of human-sensitive mediation services, blockchain-based applications need to also rely on some kind of reputation system.

C. Coexisting uses/meanings

Existing blockchain reputation systems vary widely in how reputation is earned and utilised. In many blockchain-based marketplaces, reputation does not have an explicit or software-defined role, but acts as a signal of trustworthiness. For instance, in service marketplaces (Gitcoin, Bounties Network), users can decide who to hire or work for based on transaction histories and summary statistics. Similarly, in digital goods marketplaces (Rarible, OpenSea), a buyer can review the seller's transaction history to evaluate the quality of goods for sale before making a purchase.

In blockchain-based social media (Steemit, Hive, Sapien, Relevant) and work networks (Colony, Sourcecred), reputation represents a user's evaluation weight on other users' contributions. Reputation can be global in scope or limited to a specific community or domain. Evaluation-weighting alters reputation dynamically, as users continuously influence each other's reputation scores in proportion to their own reputation. Some systems also incorporate time-based mechanisms to decay reputation with inactivity.

In blockchain-based governance frameworks (Aragon, DAOstack, Moloch), reputation often determines a user's voting weight on proposals in a given organisation. Reputation can also entitle the user to a proportional claim of the organisation's assets or ongoing revenues. Reputation is often modified through community voting, where the votes of community members are weighted by their reputation (e.g. a community can vote whether to give 50 reputation points to Alice or remove 100 reputation points from Bob). Just as in social media cases, reputation can also be modified by dynamic criteria stipulated by the community, such as reputation rewards for voting with the majority, creating proposals that pass, or reputation penalties for the reverse.

Issues currently associated with the term

A. Different types of reputation

First of all, it is important to distinguish between two different types of reputation systems: "personal" and "global" reputation systems (Hendrikx, 2015).

- **Personal reputation** systems are specific to an individual. They represent the standard mechanism of peer-to-peer reputation assignment. These systems are designed to assign a personal reputation score to each member of a particular network or community, although such a score will ultimately be relevant only to one specific individual. Hence, these systems necessarily rely on direct user input: users are expected to score each of their interactions with other community members, in order to help the system compute their corresponding reputation score. However, these systems often suffer from scalability issues. Indeed, the purpose of a reputation system is to provide information about the qualities of different users in a given domain, so that other users can make informed decisions about who they wish to interact with. Yet, a personal reputation system has limited capacity to do so, because it is not possible (or too costly) for a single user to evaluate the qualities of all the users in the system. In order to overcome this limitations, many of these reputation systems often implement a "web of trust" mechanism, leveraging the information

submitted by other people (who are regarded as trustworthy by the user) in order to compute the personal reputation score of those with whom such user did not yet have a sufficient amount of interaction.

- **Global reputation** systems are not specific to any community member, but rather to the community as a whole. These systems assign a single and unique reputation score to the different actors in a particular community or network, which will be regarded by all community members as the sole and legitimate score. These reputation systems are rather easy to implement in a centralised platform; they are much more difficult to implement in a decentralised setting, since they require highly sophisticated mechanisms of reputation transfer that will not fall prey to Sybil attacks, where anyone can create multiple pseudonymous accounts to gain disproportionate influence over the system.

It is important to note that both personal and global reputation systems suffer from specific limitations, although to different degrees. First of all, there is the problem of reputation being reduced to a single measure or score, which might not properly reflect the preferences of individual communities. Such a problem is particularly relevant in the context of global reputation systems, which are designed to average reputation into a particular score, even if values are highly heterogeneous within the community of reference. Yet, it also subsists in the context of personal reputation systems that rely on a broader web-of-trust mechanism. Second, both global and personal reputation systems might suffer from an excessive lack of granularity, to the extent that they do not differentiate between defined characteristics or properties (e.g., reputation associated with a particular skillest, as opposed to a generic reputation score). Finally—and relatedly—reputation valuations can be based on objectively quantifiable facts, as much as subjective opinions. Mixing the two can lead to misleading aggregate reputation signals.

B. Sybill attacks and identity

Unlike popular online services, decentralised systems have no central party to verify user identities, ban fake accounts, or patrol spam. While beneficial for privacy, this opens the door to Sybil attacks. While decentralised sybil-proof reputation systems have long been regarded as a theoretical impossibility (Cheng & Friedman, 2005), blockchain-based reputation systems might overcome these challenges (Almasoud et al., 2020).

One approach is to minimise the possibility of users leveraging multiple accounts by relying on centralised or decentralised identity systems—also known as "proof of personhood" (Siddarth et al., 2020). Decentralised identity systems often rely on web-of-trust models, where a small set of users slowly invites more users to be

peer-verified over time (Liu et al., 2020), or on credential-based models, where users can prove their uniqueness by collecting attestations about their identity from trusted third parties (Wang & De Filippi, 2020).

Alternatively, reputation systems can be leveraged to avoid the need of identifying users. In that model, users need to accumulate a certain degree of reputation within a particular blockchain-based system in order to influence the operation of that system (in proportion to the reputation they hold), and—potentially—assign reputation to other users of the system (Almasoud et al., 2020). Because of the proportionality between reputation and influence, an individual has to contribute just as much value, regardless of how many accounts they spread the effort over, so there is no added incentive for Sybil attacks (Pazaitis et al., 2017).

C. Privacy

In light of its attributes of transparency, censor-resistance, and immutability, blockchain technology can be instrumental to the operations of both personal and global reputation systems, enabling anyone to access and retrieve these scores, in order to compute both a personal and a global reputation score.

However, in order to protect the privacy of users, the reputation system should avoid permanently registering in a blockchain the association between real-world identities and the identities of the reputation system. In addition, users should be aware of the risks of linking real-world identities to their blockchain accounts. Maintaining this separation makes it possible for users to protect their privacy while allowing for anyone interacting within their blockchain-based identity to evaluate the risks of each user in that domain.

This is especially relevant in light of the new European General Data Protection Regulation, which provides users with the possibility to request the erasure of specific information deemed inaccurate, inappropriate, or obsolete. Given the immutability of a blockchain, the recording of any type of data that can affect the reputation of a particular persona would potentially violate the provisions of the law, insofar as the persona can be linked back to a real-world identity.

D. Oligarchies and power distribution

The use of reputation systems also raises concerns about power concentration. The creation and consolidation of oligarchies are common in online communities. However, reputation systems might reinforce inequalities in such communities, as powerful actors are more likely to be trusted and increase their reputation while

those with low reputation will have fewer opportunities to increase their reputation. Blockchain systems use reputation as a source of economic or political power: these options are explicitly made available in many governance frameworks (Aragon, DaoStack, Moloch). Thus, the accumulation of reputation in such blockchain systems might result in even stronger power inequalities than in other online communities.

E. Amplification of social inequalities

It is worth considering the potential biases reputation systems incorporate and reproduce. First, not all activities or contributions are a source of reputation in online communities (Rozas & Gilbert, 2015). Some activities, such as contributing source code in free software projects are explicitly valued in these systems, while others such as community organising, or affective labour, typically carried by women (Iosub et al., 2014) are often invisible to these reputation systems. These types of biases can trigger new forms of inequalities incorporated directly into the algorithms managing a platform, such as higher work time and lower average wage for women in the so-called gig economy (Barzilay, 2016). We have briefly considered the reproduction of gender inequalities by reputation systems. However, other dimensions of social injustice such as race or class, and their interactions, should also be considered when studying how reputation systems reproduce them.

Conclusion

Reputation in a blockchain-based system is a digital representation of an entity's standing or status in a specific domain. Reputation is usually derived from aggregated peer-evaluation of the entity's past actions. It can be leveraged both explicitly through functions in the code (voting power, economic rights) or implicitly as a means of signalling an entity's trustworthiness.

References

Ali, M., Nelson, J., Shea, R., & Freedman, M. J. (2016). Bootstrapping trust in distributed systems with blockchains. ;;*Login:*, *41*(3), 52–58. https://www.usenix.org/publications/login/fall2016/bootstrapping-trust-distributed-systems-blockchains

Almasoud, A. S., Hussain, F. K., & Hussain, O. K. (2020). Smart contracts for blockchain-based reputation systems: A systematic literature review. *Journal of Network and Computer Applications*, *170*. https://doi.org/10.1016/j.jnca.2020.102814

Barzilay, A. R., & Ben-David, A. (2016). Platform inequality: Gender in the gig-economy. *Seton Hall*

Law Rev, *47*(2), 393–431. https://scholarship.shu.edu/shlr/vol47/iss2/2

Benkler, Y. (2006). *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. Yale University Press.

Chawathe, Y., Ratnasamy, S., Breslau, L., Lanham, N., & Shenker, S. (2003). Making gnutella-like p2p systems scalable. *Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, 407–418. https://doi.org/10.1145/863955.864000

Cheng, A., & Friedman, E. (2005). Sybilproof reputation mechanisms. *Proceedings of the 2005 ACM SIGCOMM Workshop on Economics of Peer-to-Peer Systems*, 128–132. https://doi.org/10.1145/1080192.1080202

Gai, F., Wang, B., Deng, W., & Peng, W. (2018). Proof of reputation: A reputation-based consensus protocol for peer-to-peer network. *International Conference on Database Systems for Advanced Applications*, 666–681. https://doi.org/10.1007/978-3-319-91458-9_41

Hawlitschek, F., Notheisen, B., & Teubner, T. (2018). The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. *Electronic Commerce Research and Applications*, *29*, 50–63. https://doi.org/10.1016/j.elerap.2018.03.005

Hendrikx, F., Bubendorfer, K., & Chard, R. (2015). Reputation systems: A survey and taxonomy. *Journal of Parallel and Distributed Computing*, *75*, 184–197. https://doi.org/10.1016/j.jpdc.2014.08.004

Iosub, D., Laniado, D., Castillo, C., Morell, M. F., & Kaltenbrunner, A. (2014). Emotions under discussion: Gender, status and communication in online collaboration. *PloS one*, *9*(8). https://doi.org/10.1371/journal.pone.0104880

Larimer, D. (2014). *Delegated proof of stake (dpos). Bitshares Whitepaper* [White Paper].

Liu, Y., He, D., Obaidat, M. S., Kumar, N., Khan, M. K., & Choo, K. K. R. (2020). Blockchain-based identity management systems: A review. *Journal of Network and Computer Applications*, *166*. https://doi.org/10.1016/j.jnca.2020.102731

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system* [White Paper]. https://bitcoin.org/bitcoin.pdf

Pazaitis, A., De Filippi, P., & Kostakis, V. (2017). Blockchain and value systems in the sharing economy: The illustrative case of Backfeed. *Technological Forecasting and Social Change*, *125*, 105–115. https://doi.org/10.1016/j.techfore.2017.05.025

Resnick, P., Kuwabara, K., Zeckhauser, R., & Friedman, E. (2000). Reputation systems. *Communications of the ACM*, *43*(12), 45–48. https://doi.org/10.1145/355112.355122

Rozas, D., & Gilbert, N. (2015). *Talk is silver, code is gold? Contribution beyond source code in Free/Libre Open Source Software communities* (Working Paper 2015:1). Centre for Research in Social Simulation. https://cress.soc.surrey.ac.uk/web/sites/default/files/publications/working-papers/paper_contribution_beyond_source_code.pdf

Siddarth, D., Ivliev, S., Siri, S., & Berman, P. (2020). Who Watches the Watchmen? A Review of Subjective Approaches for Sybil-resistance in Proof of Personhood Protocols. *ArXiv*. http://arxiv.org/abs/2008.05300

Wang, F., & De Filippi, P. (2020). Self-sovereign identity in a globalized world: Credentials-based identity systems as a driver for economic inclusion, frontiers in blockchain. *Frontiers in Blockchain*.[

https://doi.org/10.3389/fbloc.2019.00028

Published by

Alexander von Humboldt Institute for Internet and Society

in cooperation with

CREATe

centre internet et societe

R&I IN3 Internet interdisciplinary Institute
Universitat Oberta de Catalunya