frontiers | Frontiers in Blockchain

TYPE Editorial
PUBLISHED 19 June 2023
DOI 10.3389/fbloc.2023.1235704

OPEN ACCESS

EDITED AND REVIEWED BY
Francesco Tiezzi,
Università degli Studi di Firenze, Italy

*CORRESPONDENCE
Giovanni Meroni,
giom@dtu.dk

RECEIVED 06 June 2023
ACCEPTED 14 June 2023
PUBLISHED 19 June 2023

CITATION
Meroni G, Comuzzi M and Köpke J (2023), Editorial: Blockchain for trusted information systems.
Front. Blockchain 6:1235704.
doi: 10.3389/fbloc.2023.1235704

Editorial: Blockchain for trusted information systems

Giovanni Meroni[1]*, Marco Comuzzi[2] and Julius Köpke[3]

[1]DTU Compute, Technical University of Denmark, Kgs. Lyngby, Denmark, [2]Ulsan National Institute of Science and Technology, Eonyang, Republic of Korea, [3]Alpen-Adria Universität, Klagenfurt, Austria

KEYWORDS

blockchain, information systems, trust, smart contract vulnerability, usage control

Editorial on the Research Topic
Blockchain for trusted information systems

Organizations are often required to collaborate to achieve their goals (Vandermerwe and Rada, 1988). For example, in the logistics domain, several organizations must coordinate their internal tasks to successfully deliver goods to their customers (Perboli et al., 2018). In the medical domain, various actors, such as healthcare providers, pharmacies, and insurance companies, need to collaborate to provide their services (Haleem et al., 2021). In such settings, organizations are required to exchange information in a trusted way. As some participants may be competitors, organizations must ensure to provide other partners with all and only the information required for the tasks that they are in charge of, while at the same time avoiding the leaking of confidential information. Similarly, mechanisms to ensure the provenance of the information provided, and to verify the identity of the participants, should be put in place.

Blockchain systems are a promising technology to address trust issues in information systems (Xu et al., 2019). Thanks to their distributed and decentralized nature, and their ability to reach consensus among untrusted parties, blockchains proved to be successful in supporting the exchange of digital (e.g., cryptocurrency) and possibly physical assets in a trusted way. As far as data storage is concerned, it is almost impossible for a single party or a restricted group thereof to alter or delete the information stored in a blockchain. In addition, second-generation blockchains have introduced the so-called smart contracts (Buterin, 2014), arbitrary agreements embodied by immutable code executed among multiple participants with possibly conflicting interests. Despite these features, exploiting blockchains to build trusted information systems remains far from trivial (Köpke et al., 2023).

Although the mechanisms handling the execution of smart contracts, as well as handling the data that originate from the blockchain itself, can be considered secure, the same cannot be said for the smart contracts and for the data that they receive as input. First, smart contracts may contain code vulnerabilities, which may cause unexpected behaviors and be exploited by malicious agents. For example, in 2016 a vulnerability in a smart contract allowed 3.6 million ETH to be stolen, causing the so-called DAO accident, which forced a hard fork in the Ethereum blockchain (Mehar et al., 2019). Another major issue is represented by the data originating from outside of the blockchain. Such data is not subject to the tight consistency constraints implemented within blockchains (Comuzzi et al., 2020). Consequently, with these data the blockchain alone does not provide an out-of-the-box solution to ensure traceability, persistence, and access control.

This Research Topic collects research work that aims to analyze and address the issues identified above to achieve a higher level of trust in information systems using blockchains.

To this aim, Rameder et al. perform a systematic literature review (SLR) to classify vulnerabilities, methods, analysis tools, and benchmarks that target smart contracts deployed on the Ethereum blockchain. In particular, the authors identify 10 classes of vulnerabilities and four classes of analysis methods from 195 selected publications. Then, they provide an overview of the available tools, specifying how many of them analyze a specific property of a smart contract, and make use of a specific analysis method. Finally, the authors identify five Research Topic of vulnerable smart contracts for testing, six projects that aim at analyzing vulnerabilities, but without providing any tool, and 22 tools that also provide test data to assess their efficacy. As a result of this SLR, the authors observe that—at the time when the SLR was conducted, that is, in 2021—most methods and tools focus on re-entrancy, whereas other types of vulnerabilities have received less attention. Also, a holistic taxonomy of vulnerabilities in Ethereum does not exist, and existing taxonomies mostly complement each other. Similarly, most of the available tools focus on the detection of a single vulnerability, thus requiring multiple tools to be used. Also, many tools are prone to false positives and false negatives, thus achieving neither completeness nor correctness.

The data aspect is addressed in Plebani et al., where a blockchain-based architecture permitting controlled data sharing between organizations in the context of data lakes is presented. This architecture allows to uphold data sovereignty while supporting data analytics. The architecture leverages the traceability and accountability features of blockchain to oversee the data-sharing processes. It facilitates the ingestion of external organizational data while also enabling sharing of internal data, all within the strict boundaries of data sovereignty rules. Additionally, it allows for balancing computational and data movements in a federated environment by using containers. This approach has been applied in a healthcare setting where clinical data is collected and stored in local data lakes across various entities such as hospitals, research institutes, and medical universities. This study highlights the potential of combining blockchain with data analytics, showcasing a promising path to navigate the intricacies of data sharing and sovereignty for data analytics.

Basile et al. tackle both trusted execution and data by proposing a framework to facilitate usage control in decentralized Web environments. Specifically, the proposed approach addresses the limitations of decentralization initiatives such as Solid, Digi.me, and ActivityPub, which use access control mechanisms that cannot verify compliance with usage conditions after access has been granted to external actors. To address this issue, the authors propose a resource governance conceptual framework, named ReGov, that specifically facilitates usage control in decentralized Web environments. The conceptual framework can be then instantiated using a combination of blockchain technology and trusted execution environments. Blockchain, in particular, is required to record immutable policies expressing the usage conditions associated with resources and monitor their compliance. The trusted execution environments enforce these policies inside data consumers' devices.

Author contributions

GM, MC, and JK are the topic editors. GM wrote the first draft of the manuscript. All authors contributed to the article and approved the submitted version.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

References

Buterin, V. (2014). Ethereum: A next-generation smart contract and decentralized application platform.

Comuzzi, M., Cappiello, C., and Meroni, G. (2020). On the need for data quality assessment in blockchains. *IEEE Internet Comput.* 25, 71–78. doi:10.1109/mic.2020.3030978

Haleem, A., Javaid, M., Singh, R. P., Suman, R., and Rab, S. (2021). Blockchain technology applications in healthcare: An overview. *Int. J. Intelligent Netw.* 2, 130–139. doi:10.1016/j.ijin.2021.09.005

Köpke, J., Meroni, G., and Salnitri, M. (2023). Designing secure business processes for blockchains with secbpmn2bc. *Future Gener. Comput. Syst.* 141, 382–398. doi:10.1016/j.future.2022.11.013

Mehar, M. I., Shier, C. L., Giambattista, A., Gong, E., Fletcher, G., Sanayhie, R., et al. (2019). Understanding a revolutionary and flawed grand experiment in blockchain: The dao attack. *J. Cases Inf. Technol. (JCIT)* 21, 19–32. doi:10.4018/jcit.2019010102

Perboli, G., Musso, S., and Rosano, M. (2018). Blockchain in logistics and supply chain: A lean approach for designing real-world use cases. *IEEE Access* 6, 62018–62028. doi:10.1109/ACCESS.2018.2875782

Vandermerwe, S., and Rada, J. (1988). Servitization of business: Adding value by adding services. *Eur. Manag. J.* 6, 314–324. doi:10.1016/0263-2373(88)90033-3

Xu, X., Weber, I., and Staples, M. (2019). *Architecture for blockchain applications*. Germany: Springer.