A New Blockchain Ecosystem for Trusted, Traceable and Transparent Ontological Knowledge Management

Position Paper

Thanasis G. Papaioannou[1], Vlado Stankovski[2], Petar Kochovski[2], Anthony Simonet-Boulogne[3], Caroline Barelle[4], Alberto Ciaramella[5], Marco Ciaramella[5], and George D. Stamoulis[1]

[1] Athens University of Economics & Business (AUEB), Greece
{pathan,gstamoul}@aueb.gr
[2] University of Ljubljana, Slovenia
{Vlado.Stankovski,Petar.Kochovski}@fri.uni-lj.si
[3] iExec, France asb@iex.ec
[4] European Dynamics, Luxembourg caroline.barelle@eurodyn.com
[5] IntelliSemantic, Rivoli, Italy
{alberto.ciaramella,marco.ciaramella}@intellisemantic.com

Abstract. The Internet is becoming more centralized, more asymmetric in terms of knowledge and power distribution, more biased, less privacy-preserving and less trustworthy. Blockchain technologies already enable the safe and fair exchange of digital assets in a decentralized manner; however, its application to information exchange remains largely unexplored. This article exposes our vision for a semantically-enriched blockchain software ecosystem named ONTOCHAIN, that enables the development of trustworthy distributed applications that can empower users, guarantee both their privacy and high quality of service, and ultimately support pluralism and democracy. ONTOCHAIN aims primarily to attain trustworthy service exchange and trustworthy content handling by means of advanced knowledge management mechanisms for several domains such as health, economy, public services, energy and sustainability, news, media, entertainment, Industry 4.0 and tourism. We present the main components of the ONTOCHAIN architecture and their functionality. Finally, the validity of our approach is exemplified by describing how decentralized applications can be enabled by the ONTOCHAIN ecosystem.

Keywords: Trust · E-commerce · Anonymity · Smart Contract · Decentralized Apps.

1 Introduction

The success of the Internet lies in free speech, open innovation and interoperability. However, there are growing concerns that openness, trustworthiness, privacy

and security are being threatened by the seek of high performance and profit. More specifically, multiple threats have been identified when people interact with online services: centralization of power (i.e., information and knowledge being in the hands of only few actors), unknown provenance of information (e.g., fake news), anonymity in favor of criminal activity, personal privacy violations and personal data exploitation (e.g., Cambridge Analytica scandal), biases in AI algorithms (e.g., under-representation of certain social groups in training data can make AI algorithms discriminate against those social groups), no fair rewards for quality contributions (e.g., provision of credible reviews), and more threaten the fundamental rights of users.

Decentralization is a key property enabled by Distributed Ledger Technologies (DLT), such as blockchain [13]. Blockchains are "trustless", i.e., the mechanisms in place allow all parties in the system to reach a consensus on what the normative truth is without requiring any trust in any third party. Thus, the various stakeholders of the network (e.g., developers, miners, and consumers) share power and trust, instead of placing it to a single individual or entity (e.g., banks, governments, and financial institutions). However, so far, blockchain does not deal with identity management, trustworthiness assessment of data and entities, trustworthiness of data handling, smart contracts that understand data semantics, secure data exchange or secure storage. Moreover, while being run on a shared decentralized infrastructure, it suffers from the Scalability Trilemma, a term coined by Vitalik Buterin (founder of Ethereum), that refers to the trade-offs among decentralization, security and scalability that crypto projects must make when deciding how to optimize the underlying architecture of their own blockchain.

In this paper[6], we describe our vision to shape a multi-layer and modular blockchain framework, to enable the implementation of a number of different next-generation real-world solutions, such as trustworthy web and social media, trustworthy crowdsensing, trustworthy service orchestration, unsupervised, decentralized online social networks, etc. and to empower practitioners to address the various challenges of the Internet (e.g., centralization of power and knowledge, unknown provenance of information, anonymous and unreliable identifiers, personal data exploitation, AI biases, data censorship, fraud, etc.) through the use of multiple ledger and semantic technologies. Our use-cases are intended to be built upon different protocols and interactions among different blockchain components. The proposed blockchain-based framework is expected to enable higher performance and scalability, through the engagement of different business logic, access methods and governance models, whereas to present scalable solutions for ensuring secure and transparent content and information exchange as well as service interoperability. Moreover, our use-cases will rely on successful Semantic Web approaches such as Linked Data, OWL Lite, OWL DL and other approaches and formats that will deliver a trustworthy, privacy-preserving, secure, transparent, democratic and traceable approach to manage access and operations over ontologies, metadata, data, knowledge and information in the ecosystem. Our technology framework will constitute a building block of the next

generation Internet towards a more human-centric Internet that supports values of openness, decentralisation, inclusiveness and protection of privacy as well as giving the control back to the end-users to be able to benefit from democratic, transparent and trustworthy decision making mechanisms.

The remainder of this paper is organized as follows: In Section 2, we overview the background and related work. In Section 3, we describe our approach towards a semantically-enriched, trustworthy blockchain ecosystem. In Section 4, we overview the architecture of our framework under development and describe its main component. In Section 5, we exemplify how our technological framework enables promising use-case scenarios that tackle fundamental user needs. Finally, in 6, we conclude our work and outline future work.

2 Background and Related Work

Blockchains became popular in 2008 after Satoshi Nakamoto released the Bitcoin white paper [13], but their applications span far beyond monetary transactions; energy, mobility, logistics, supply chain, healthcare and insurance are just a few domains that drive the growth of Distributed Ledger Technologies and make it one of the most important trends in the IT industry. A blockchain is a append-only ledger of records, grouped into blocks after validation by a distributed consensus across the networks participants [9,15]. Each block typically contains a timestamp, a cryptographic hash value of the previous block and a sorted list of validated transactions. This technology builds on a combination of older technologies, e.g. peer to peer protocols, cryptographic primitives, distributed consensus algorithms and game theory. As such, the blockchain is more of a paradigm shift in the way networked applications will be built, deployed, operated, consumed and marketed than just a technology. Unlike Bitcoin which supports only simple value transfers, modern blockchains like Ethereum [19] support *smart contracts*, i.e., self-executing decentralized programs that can read and write the state of the blockchain on top of which they are deployed. Smart contracts [6] enable the specification of advanced logic and the automation of business workflows. Whereas programs used to imply trust in one or several third parties from its user, a smart contract is transparent by design: its result (i.e., the new state of the blockchain) requires a consensus of the participants, and once committed on the ledger, it cannot be forged. Depending on implementation and deployment choices, many other key properties can be insured, e.g., the resistance to censorship and tampering, pseudo-anonymity, fault-tolerance, resilience, and non-repudiation.

In this context, blockchains are foreseen as the core backbone of novel, large, inter-connected environments such as smart cities and IoT applications where security and trust in information and data processing services are paramount to adoption and to the respect of users rights. So, the suitability of blockchain technologies has been demonstrated in numerous works [11], e.g., for the management of medical records [12], for notary [16] and public services [17], identity [20] and reputation [7] and data traceability [18]. Several initiatives are aiming to

bring the benefits of DLTs to different business domains in an attempt to disrupt virtually every aspect of life. GAIA-X [2] is building a European data infrastructure for developing innovative trustworthy and sustainable data economy, by relying on standards and open-source software. The project federates services from participating providers within one user-friendly ecosystem which supports federated entities, access-control and privacy-preserving processing by design. Hyperledger Fabric [4] (HLF) is a permissioned blockchain project originally developed by IBM and distributed as free software. HLF follows a flexible modular design which allows to simply replace components (e.g. consensus, smart contract language) and adapt to various application domains. Although HLF has demonstrated fast transaction throughput, its limited scalability to a maximum of about 16 peers [14,8] and its vulnerability to compromised nodes [5] limits its applicability to small to medium enterprise consortiums. The exploitation of Hyperledger Fabric as SaaS by IBM[7] contributes to its adoption by a large variety of industries to deploy entreprise blockchain networks. EOSIO [1] offers a modular framework for creating industrial-scale permissioned or permissionless blockchains and implements a 2-layer consensus protocol which combines a Byzantine Fault Tolerant protocol and a delegated Proof-of-Stake protocol. According to its developers, EOSIOs protocol allows the chain to achieve up to 8,000 Transactions Per Second, way ahead of Hyperledger Farbic [8], although no scientific evaluation of EOSIOs performance have been conducted.

ONTOCHAIN considers several challenges to unlock the tremendous potential of blockchain technology and make it technically, economically and legally viable in business environments for ensuring trust and accountability in information sharing and data processing. The first set of challenges are technical ones; although several solutions partly address the topics of identity, privacy-preserving data processing, trustworthy information handling and data provenance, no blockchain ecosystem supports web semantics natively and enables the development of information-centric applications like ONTOCHAIN intends to. The second set of challenges is related to the development of viable business models and incentives, i.e., creating an environment of peers that all profit from fair data production and data usage and makes unfair or malicious behavior unprofitable. The last sets of challenges are of legal nature; sitting at the intersection of finance and data processing, ONTOCHAIN must incorporate the recent General Data Protection Regulation as well as upcoming and quickly changing regulations aimed at strengthening the privacy of citizens within the EU.

3 The Vision and Approach

Today, the Internet is involved in all aspects of our lives. With the number of services available constantly on the rise, we are witnesses to an ever-increasing information overload. In addition, poor content aggregation mechanisms and

[7] https://www.ibm.com/blockchain

stovepipe systems are making effective collaboration and smart decision making an even bigger challenge.

Notwithstanding the ability of advanced technologies to distinguish factual from non-factual data, existing large or small WWW services are used today with the purpose of spreading misleading information that usually serve a certain purpose: to damage ones reputation, win an election, make people buy products and services. With the confluence of the WWW with the Internet of Things, the ubiquitous Artificial Intelligence, the existence of Cloud, Fog and Edge computing platforms and similar, it becomes apparent that the existing problems of misuse of information can soon achieve even more dangerous levels of potential manipulation of the people that must be prevented.

As a response to these challenges a new vision has arisen. A vision where Internet (WWW, social networks, social media and IoT, etc.) data are understood by the machines and made accessible to an array of semantic technologies, therefore allowing the machines to do more effective and value adding work when responding to service requests.

Technically, this is achieved by using ontologies, that is, "formal, explicit specification of shared conceptualizations". Ontologies make it possible to intertwine the data and information into a Web of Knowledge. Several successful companies have built on the Semantic Web ideas in the past decades and have had enormous success, with the most popular applications being in the form of knowledge graphs such as Google Knowledge Graph or IBM Socrates. However, the Semantic Web does not execute uniformly for all. In such a system actors can sometimes make completely opposed assertions, such as "that apple is red and "that (same) apple is yellow. This concept becomes especially important in crowdsensing which allows anyone to contribute the data acquired by their own connected objects in order to build collaborative knowledge. What is currently necessary, is to be able to establish the truth from several assertions.

With the emergence of the Internet of Things (IoT), the new wave of Artificial Intelligence (AI), Orchestration and novel Cloud Continuum approaches (Edge, Fog, Data Center), we now have the potential to reach a new level of decentralization, but also of cooperation between various cyber-physical systems based on the Semantic Web principles. Blockchain technologies with their main properties of decentralisation, traceability and transparency fit perfectly to this agenda, and may contribute to achieving trusted operations of such smart applications and systems [10]. The hypothesis of this work is that with these intrinsic properties of blockchain, it is possible to establish a common, shared ledger for the management of shared ontological concepts including instances of such concepts. An important aspect of ONTOCHAIN is the ability to interlink off-chain data, information and (AI) services with on-chain information in a way that reduces the need for costly on-chain operations and provides significant new properties, such as traceability, privacy, mechanisms for democracy and other.

Membership of different entities (e.g. specific objects, persons), in specific ontological concepts can be established, for example, by means of independent evaluation of various stakeholders with the use of AI methods. These entities

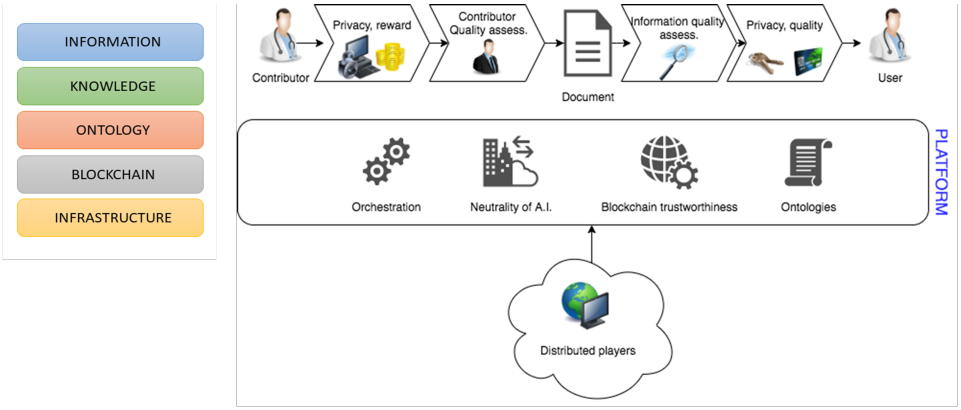

Fig. 1. Our vision and approach.

can be anonymous, but at the same time, they are able to be linked to real-word identities, when law demands it. Not only ontological concepts may be well-agreed among the participants, but also they can be directly "executable" through the employment of various semantic reasoners, operating directly on blockchain, potentially also employing trustworthy offchain real-world data (e.g., IoT) with the use of Smart Oracles and Decentralized Oracles that establish facts by using democratic, decentralised means. Overall, ONTOCHAIN's vision is depicted in Fig. 1, where trustworthy services, data and knowledge are exchanged in privacy-aware and traceable manner based on a layered approach on top of a semantically-enriched distributed ledger infrastructure.

4 The Architecture

A multi-layer approach to reach the envisioned ONTOCHAIN framework and to serve the defined use-cases and applications is followed as described in Figure 2. This framework will enable the implementation of a number of innovative different next-generation real-world solutions, such as trustworthy web and social media, trustworthy crowdsensing, trustworthy service orchestration, unsupervised/decentralized online social networks, etc. Eventually, we predict that the diversity, the complexity and the specialization of different real-world ONTOCHAIN applications will lead practitioners to use multiple ledger technologies for implementing different solutions. This will enable higher performance and scalability, while enabling different business logic, access methods and governance models that require specific chains. ONTOCHAIN use-cases will be built upon the different protocols shown in Figure 2. It is important to note that most of the components of the proposed architecture do not exist into any of the competitive platforms mentioned in Section 2. ONTOCHAIN Application and Core

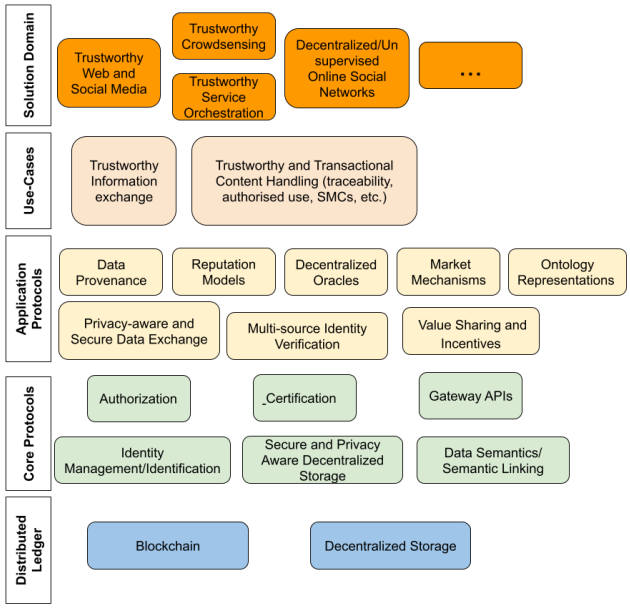

Fig. 2. The ONTOCHAIN architectural framework.

protocols will implement the interactions between different blockchain frameworks, while hiding them from the use-cases to support effortless inter-service process cooperation. Moreover, data stored at different chains, may be linked together. This linkage will be stored in new ONTOCHAIN chains.

For enabling scalability, openness and high performance, we employ a modular approach. Each of the modules and functionality of each layer is built upon functionality offered by the lower layers. The functionality of the modules at each layer is described in a top-down manner below, along with the dependencies among them.

Use-Case Layer

Trustworthy Information Exchange: This use case encapsulates the tools and libraries for the secure exchange of trustworthy data among trustworthy parties. It employs and combines data provenance mechanisms, decentralized oracles and user trustworthiness to assess trustworthiness of information. Decentralized reputation models are employed to assess the trustworthiness of data sources and that of the data itself, while the secure data exchange mechanisms are employed to transfer the data securely among transacted parties through cryptographic mechanisms.

Trustworthy and Transactional Content Handling: This use case enables trustworthy data handling by means of any combination of the following: authorized

access/handling of the data, data credibility assessment, implementation of copyrights, secure and privacy aware querying of the data (e.g., by means of secure multiparty computation and data sanitization approaches). This use case also deals with the secure transfer of any financial assets among involved parties in a data transaction. Regulatory alignment of data transactions, as a part of Trustworthy and Transactional Content Handling, will define and develop tools and mechanisms that would allow regulatory, judiciary and law enforcement agencies to introspect and otherwise influence data transactions in strictly defined circumstances envisioned by legislature.

Application Protocols Layer

Data Provenance: This module will provide graphical and programming interfaces for querying and presenting provenance information from ONTOCHAIN about on-chain and off-chain data. Provenance information will include the complete trail of transactions that resulted in a record.
Reputation Models: This module will provide the functionality of building different decentralized reputation models over the blockchain, so that reputation feedback is genuine, credible and anonymous. This module is built upon Identity Verification mechanisms.
Decentralized Oracles: This module will facilitate Smart Contracts to operate with off-chain data, although by design, Smart Contracts can only read and write data that is stored on their blockchain. To avoid centralization, some approaches (e.g. Substrate, ChainLink) apply multiple instances to look at a data source, and then run a consensus algorithm on-chain to validate the result. This, however, only displaces the point of centralization from the Oracle to the data source. While the idea of Decentralized Oracles is simple, its implementation is not trivial: every use-case requires different data sources, and the consensus algorithm based on multiple data types can become complex.
Market Mechanisms "as a Service: This module provides the basic support mechanisms for enabling data/service transaction, and thus enables market mechanisms. For example, this module will support trading of physical assets (e.g., tokenization) and price determination (e.g., auctions, negotiation protocols, etc.), billing, customer support, inventory management services and more. It also provides functionality for enabling the sharing economy, such as value chaining, value/cost sharing and DeFi support.
Secure Data Exchange: This module comprises the functionality of exchanging data among distributed parties, while verifying the ownership of the data and access rights, authenticity of transacted parties, the integrity of the data exchanged and the confidentiality of the data through blockchain underlying mechanisms. Most often, off-chain data will be exchanged in data transactions, while on-chain data will store public cryptographic keys and access control lists based on which elevated data access to different portions of data is authorized for specific transacted parties.
Ontology Representation: This module seeks to define new ways for implementing ontologies with the use of blockchain. Semantic agreements can be commonly

agreed based blockchain-based consensus, similarly to the establishment of axiomatic statements. Moreover, new ontologies will be defined for smart contracts and decentralized services to enable service searchability and matching with service requests. This module will also include any reasoning approaches, tools and methods that can help deduce new knowledge arriving from a sensing IoT empowered environment.
Multi-source Identity Verification: This module seeks to register and verify individual digital identities of physical objects via newly designed ONTOCHAIN services. For instance, various AI methods could be introduced to operate on sensing data (IoT based, sensors, cameras and similar) to assert whether an individual belongs to a specific ontological concept.
Value Sharing and Incentives: ONTOCHAIN ecosystem is to be, by nature, a public good built upon the resources and efforts of a great number of people. Proper incentive mechanisms for rewarding the people involved, according to their contribution, should be in place. Such mechanisms could include: i) the generation of a certain number of cryptocurrencies for block mining and execution of smart contracts, ii) contribution assessment.

Core Protocols

Certification: This module refers to the confirmation of certain characteristics of an object, person, or organization. For example, a government may decide to offer certificates to cloud providers that have verified GDPR-compliant handling of private citizens data [3]. In such case, certificates can be issued on-chain (i.e. implemented within Smart Contracts), and can be used as conditions for performing specific transactions, for example, using AI methods to analyse private data.
Secure/Privacy Aware Storage: This module encapsulates solutions already existing on blockchain. Together with decentralisation they help reduce the risk of one party having access to all private data. Moreover, various partitioning, fragmentation and redundancy methods will be used (e.g., StorJ).
Identity Management: This module deals with technologies and solutions to address parts of the digital identity puzzle. There are two conflicting requirements that drive this development: i) ability to identify oneself in specific interactions (e.g., withdrawing money in a bank), ii) preservation of ones privacy (e.g., healthcare data, online buyers habits).
Gateways/Bridges: This module will support connections between the ONTOCHAIN blockchain and the outside world, including other blockchains in the form of Smart Contracts, as well as several higher-level wrappers for commonly used languages (e.g. JavaScript, Java and Python). Our prototype will be implemented using the Ethereum software stack, because of its important community of adopters and developers.
Data Semantics: Since ontology engineering is a complex work that usually takes many years to complete and test, this module intends to stimulate reuse of this body of generated knowledge in order to foster the use of various schemata and

ontologies when describing the semantics of data. Ontologies are core building block of the Semantic Web [https://www.w3.org/]. The W3C consortium provides mechanisms for their standardisation in order to foster their use in applications world-wide, with the potential to build various artificial agents that can cross-link the information, and perform advanced queries via SPARQL. Supporting these standards in the blockchain and providing data semantic annotation, semantics extraction, linking, inference, alignment and reasoning on top of blockchains will significantly boost the business viability of future applications involving knowledge management.
Authorisation: Blockchain has stimulated the idea of self-sovereign digital identity. Various Role-Based Access Control (RBAC) systems have also existed for decades. With this module, one could easily see systems where a patient is self-identified on blockchain, while a medical doctor gains access to the medical records based on her/his role (e.g., surgeon, general practitioner).

Distributed Ledger

Blockchain Consensus Engine: Consensus making mechanisms are at the core of any blockchain. ONTOCHAIN will be designed to be scalable, open, cost and energy-efficient, and when possible even as a much improved new consensus engine. Regarding openness, ONTOCHAIN does not aim for a silo blockchain ecosystem, but for an open distributed ledger that in principle can be combined with different blockchain environments.
Decentralised Storage: Various decentralised repositories, such as Peer-to-Peer and Content Distribution Networks have existed for decades. With the emergence of blockchain, we have witnessed a new wave of participatory storage repositories that can help address the security and privacy needs, and may help store practically any kind of data (e.g., StorJ). In the near future, one could imagine new storage services, that can help store private data in encrypted and decentralised way, that can help manage data replicas for reliability and Quality of Service, while balancing the trade-offs with the storage costs.

5 Use Cases

ONTOCHAIN will enable many forthcoming applications, from B2B to C2C to G2C, in different verticals, including:

- Arts - Remunerate artistic work
- Commerce and Trading P2P eCommerce - Proprietary data trading
- Education - Credible and authentic eScience
- Finance - Decentralized borrowing and lending
- Healthcare Access to patient data Drug control Privacy-aware data analytics
- Industry - Privacy-aware data analytics
- Insurance - Decentralized, Transparent and Trustworthy Insurance

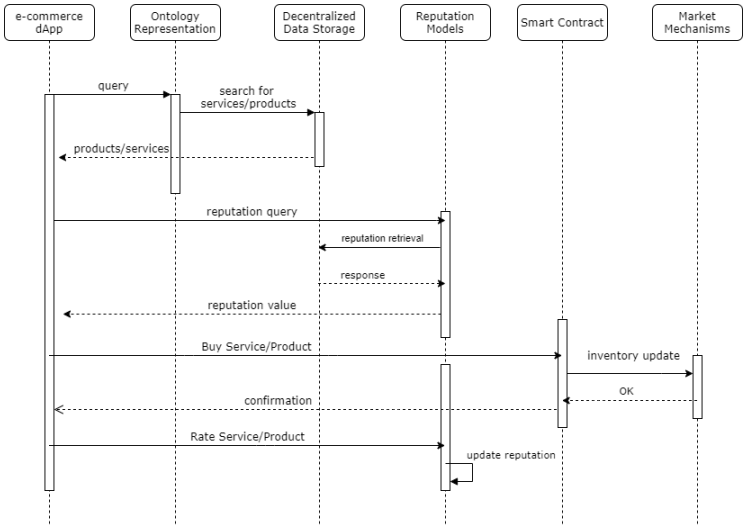

Fig. 3. P2P commerce distributed application scenario.

– Manufacturing Supply Chain Management Maintenance tracking
– Public Sector Smart cities Traffic control

A use-case scenario related to P2P e-commerce is detailed as example hereafter. In this use case, users are able to search for products/services provided by business entities based on data semantics. Users receive the matching product/service from the most reputable provider. The product/service transaction is then recorded in the blockchain as well as the changes of ownership of the product or the access provision to a service. In parallel, the product/service is removed from the inventory of the seller and an invoice is automatically issued. Finally, users may submit rating data on their past transactions. Fig. 3 summarizes the main interactions of this application.

Another use-case scenario concerns prorpietary-data trading. Individuals or data aggregators collect personal/proprietary data that are subject to privacy concerns and their handling is governed by GDPR. In this application, data is securely stored, uniquely identified and access to it is restricted to authorized entities for pre-specified handling. Data handling can be realized in secure enclaves through predetermined algorithms, also part of the smart contract, without any disclosure of the original data to any third party. The validity of the smart contract against GDPR is automatically validated and any processing activities to the data are recorded in the blockchain. Any data transformations that produce new data, are being treated as tradeable assets, while their provenance can be established based on their link to the original data (which has not been disclosed) and the processing algorithms.

6 Conclusion

In this paper, we presented an overview of the challenges of todays Internet, and how ONTOCHAIN platform by combining ontological knowledge and blockchain technology plans to tackle them. We described the architecture and the main functionality of our innovative blockchain ecosystem. Moreover, using two use case scenarios, we exemplified how the proposed platform enables innovative and promising distributed applications. As a future work, we plan to define the ONTOCHAIN architecture in more depth with detailed APIs among the different components and implementation details. Additionally, we will demonstrate prototype implementations of exemplary distributed applications enabled by the proposed platform.

Acknowledgements. The research and development reported in this paper have received funding from the European Union's Horizon 2020 Research and Innovation Programme under grant agreement no. 957338 (ONTOCHAIN: Trusted, traceable and transparent ontological knowledge on blockchain).

References

1. EOSIO Dawn 3.0 Now Available. https://medium.com/eosio/eosio-dawn-3-0-now-available-49a3b99242d7, accessed: 2021-06-15
2. GAIA-X: A Federated Data Infrastructure for Europe. http://www.data-infrastructure.eu/GAIAX/, accessed: 2021-06-15
3. General Data Protection Regulation. https://gdpr-info.eu/
4. Hyperledger Fabric Homepage. https://www.hyperledger.org/use/fabric, accessed: 2021-06-15
5. Bhuvana, R., Aithal, P.: Blockchain based Service: A Case Study on IBM Blockchain Services & Hyperledger Fabric. International Journal of Case Studies in Business, IT, and Education (IJCSBE) **4**(1), 94–102 (2020)
6. Christidis, K., Devetsikiotis, M.: Blockchains and smart contracts for the internet of things. Ieee Access **4**, 2292–2303 (2016)
7. Dennis, R., Owen, G.: Rep on the block: A next generation reputation system based on the blockchain. In: 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST). IEEE (2015)
8. Dinh, T.T.A., Wang, J., Chen, G., Liu, R., Ooi, B.C., Tan, K.L.: Blockbench: A framework for analyzing private blockchains. In: Proceedings of the 2017 ACM International Conference on Management of Data (2017)
9. Hamida, E.B., Brousmiche, K.L., Levard, H., Thea, E.: Blockchain for enterprise: overview, opportunities and challenges. In: The Thirteenth International Conference on Wireless and Mobile Communications (ICWMC 2017) (2017)
10. Kochovski, P., Gec, S., Stankovski, V., Bajec, M., Drobintsev, P.D.: Trust management in a blockchain based fog computing platform with trustless smart oracles. Future Generation Computer Systems **101**, 747–759 (2019)
11. Maesa, D.D.F., Mori, P.: Blockchain 3.0 applications survey. Journal of Parallel and Distributed Computing **138**, 99–114 (2020)

12. Mettler, M.: Blockchain technology in healthcare: The revolution starts here. In: 2016 IEEE 18th international conference on e-health networking, applications and services (Healthcom). IEEE (2016)
13. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system. Bitcoin White Paper (2008 [Online]), https://bitcoin.org/bitcoin.pdf
14. Nasir, Q., Qasse, I.A., Abu Talib, M., Nassif, A.B.: Performance analysis of Hyperledger Fabric platforms. Security and Communication Networks **2018** (2018)
15. Singh, K., Heulot, N., Hamida, E.B.: Towards anonymous, unlinkable, and confidential transactions in blockchain. In: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE (2018)
16. Song, G., Kim, S., Hwang, H., Lee, K.: Blockchain-based notarization for social media. In: 2019 IEEE international conference on consumer electronics (icce). pp. 1–2. IEEE (2019)
17. Sullivan, C., Burger, E.: E-residency and blockchain. computer law & security review **33**(4), 470–481 (2017)
18. Tian, F.: An agri-food supply chain traceability system for china based on rfid & blockchain technology. In: 2016 13th international conference on service systems and service management (ICSSSM). IEEE (2016)
19. Wood, G., et al.: Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper **151**(2014), 1–32 (2014)
20. Yasin, A., Liu, L.: An online identity and smart contract management system. In: 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC). vol. 2. IEEE (2016)