Multi-Agent Systems and Blockchain: Results from a Systematic Literature Review

Davide Calvaresi[1,2,*], Alevtina Dubovitskaya[1,3,*], Jean Paul Calbimonte[1], Kuldar Taveter[4], and Michael Schumacher[1]

[1] University of Applied Sciences and Arts Western Switzerland, Sierre, Switzerland,
[2] Scuola Superiore Sant'Anna, Pisa, Italy
[3] Swiss Federal Institute of Technology, Lausanne, Switzerland
[4] Tallinn University of Technology, Tallinn, Estonia
[*] the authors share an equal contribution
{name.surname}@hevs.ch, kuldar.taveter@ttu.ee,

Abstract. Multi-Agent Systems (MAS) technology is widely used for the development of intelligent distributed systems that manage sensitive data (e.g., ambient assisted living, healthcare, energy trading). To foster accountability and trusted interactions, recent trends advocate the use of blockchain technologies (BCT) for MAS. Although most of these approaches have only started exploring the topic, there is an impending need for establishing a research road-map, as well as identifying scientific and technological challenges in this scope. As a first necessary step towards this goal, this paper presents a systematic literature review of studies involving MAS and BCT as reconciling solutions. Aiming at providing a comprehensive overview of their application domains, we analyze motivations, assumptions, requirements, strengths, and limitations presented in the current state of the art. Moreover, discussing the future challenges, we introduce our vision on how MAS and BCT could be combined in different application scenarios.

Keywords: Multi-Agent Systems, Blockchain, Systematic Literature Review

1 Introduction

Technological revolutions have deeply changed habits and customs in contemporary society. Everyday items such as smartphones, cars, clothes and household appliances are gaining increasingly sophisticated computing and communication capacities, becoming irrevocably present in everyday life. In domains such as e-health, assisted living, tele-rehabilitation, manufacturing, zero-energy buildings, near-zero automotive fatalities, ubiquitous computing is dramatically rising, thus demanding the scientific research to push towards devices that autonomously collaborate/compete with each other [1,2]. Most of these decentralized systems implement a sort of distributed intelligence, in many cases emulating humankind dynamics. For example, in the last decades, Multi-Agent Systems (MAS) gained a crucial role in the development of intelligent distributed systems, often exchanging sensitive data [3]. In this context, accountability and trusted interactions among agents have become mandatory aspects, which entail a number of

technical and scientific challenges. Despite many attempts and previous works aiming at developing models and mechanisms to guarantee communications security and trust in MAS [4,5,6], such requirements have not been fully satisfied yet.

Recent trends [7,8,9,10] nourish the promising idea of integrating MAS and blockchain technologies (BCT) [11,12], with the expectation of providing BCT features in use-cases where agent systems require them. However, employing a new technology such as blockchain "as-is" and by itself in dynamic and quickly evolving scenarios can represent an unlucky choice. This may be due to several reasons, spanning from fundamental properties of BCT, to application/domain specific constraints. As an example, consider the modification of blockchain code, which can happen through majority consensus. Reaching consensus in a distributed multi-stakeholder network with possible unaligned interests can be considerably complex, and new issues might be introduced as a result [13]. Although effective, some strategic decisions can hinder the evolution of the technology from academic institutions to real-world problems [14].

Nevertheless, combining BCT and MAS can represent a win-win solution if properly managed: On the one hand, the adoption and adaption of BCT may fix the security limitations broadly known in MAS literature. On the other hand, BCT can also contribute with features missing in some MAS scenarios (e.g., flexibility). For example, cloud computing systems dealing with potentially "very large datasets" are going towards a process of *agentification*, exploiting the crucial support of blockchain technology [8]. Considering agents as atomic entities populating P2P communities, the design of a fair scheduling and a general protection of the whole cluster against abusive or malfunctioning nodes is currently one of the main challenges [15]. In particular, in distributed master-less systems with reputation rating across the cluster, the application of multi-level principles of cryptocurrencies has given insightful results [15]. In fact, in [14] it is demonstrated that by combining peer-to-peer networks with cryptographic algorithms a group of agents can reach an agreement on a particular state of affairs and record that agreement, without the need for a controlling authority. The combination of blockchain and MAS in any distributed-like scenario (e.g., swarm robotics [14]) can provide the necessary capabilities to make distributed entities operations more secure, autonomous, flexible and even profitable.

A number of other examples in the literature show the recent interest in using BCT to address different challenges already present in MAS, and in various application domains. The intuition behind the integration of these paradigms and their underlying technologies is mainly driven by the needs of including features such as integrity, identity management, provenance, transaction guarantees, data security, to name a few. However, many of the implications of the results of this integration remain to be assessed. Moreover, there is a need for assessing where the combination of BCT and MAS is adequate, and what are the new challenges that arise by connecting them.

The **contribution** of this work is three-fold: (i) To better understand the motivations and the relevance of the existing contributions that combine MAS and BCT, it develops a *Systematic Literature Review (SLR)* of the current state of

the art, capturing the application domains, motivations, assumptions, strengths and limitations. (ii) It *analyzes the correctness and justification* of using BCT to address the requirements of MAS. (iii) It *formalizes the open challenges* of applying BCT in practice, in particular in the framework of MAS, and *provides directions for future research.*

The paper is organized as follows: Section 2 introduces basic concepts, Section 3 presents the review process and data collection, Section 4 organizes and describes the obtained results, Section 5 discusses the obtained results, lists open challenges, and details several application scenarios, for which coupling BCT and MAS would be highly beneficial. Finally, Section 6 concludes the paper and presents possible future works.

2 MAS and BCT: Basic Concepts

2.1 Principles of MAS

An agent can be rationalized as an autonomous entity, with an expendable knowledge, driven by self-developed or induced objectives [16]. Moreover, agents can observe the surrounding environment through a perception layer, and possibly interact with it, as well as with other agents. MAS are generally composed of loosely coupled agents interconnected and organized in a network. The degrees of cooperation among agents, the type of application, and agent interaction model generate a broad range of behaviors. These may include concepts related to knowledge (data) sharing among agents, message-passing strategies, agreement and consensus, reputation and trust among agents, voting systems, agent identity management, and many more.

Regardless distribution and dimensions, although broadly appreciated, MAS autonomy and flexibility still generate minor concerns about possible evolution in undesired behaviors of inferences and plans. Moreover, depending on the cooperative/competitive nature of the community factors such as *trust* and *reliability* are still open challenges heavily affecting the MAS pillars: *(i)* agent local scheduler, *(ii)* communication protocol, and *(iii)* negotiation protocol [3,17].

2.2 Principles of Blockchain

Blockchain is a peer-to-peer distributed ledger technology that provides a shared, immutable, and transparent append-only register of all the actions that have happened to all the participants of the network. It is secured using cryptographic primitives such as hash function, digital signature, and encryption [18]. The data in the form of transactions, digitally signed and broadcasted by the participants, are grouped into the blocks in the chronological order and timestamped. A hash function is applied to the content of the block and forms a unique block identifier, which is stored in the subsequent block. Due to the properties of the hash function, (result is deterministic and can not be reversed) it could be easily verified if the content of the block was modified by hashing the block content again and comparing it with the identifier from the subsequent block. The blockchain

is replicated and maintained by every participant. With this decentralized approach there is no need for setting up a trusted centralized entity for managing the registry. A malicious attempt to tamper the information stored in the registry will be noticed by the participants, thus guaranteeing immutability of the ledger. Many blockchains can execute arbitrary tasks, typically called smart contracts[5], written in a domain-specific or a general-purpose programming language [19].

To add a new block to the ledger a *consensus* protocol is employed [20]. Based on how the identity of a participant and its right to participate in the consensus are defined within a network, one could distinguish between public and private, permissioned and permissionless blockchain systems. In a permissionless blockchain, such as Bitcoin [18] or Ethereum [21], anyone can can join the network, anyone can "write" to the shared state through invoking transactions (provided transaction fees are paid for), and anyone can participate in the consensus process for determining the "valid" state. Permissionless (or "public") blockchains are coupled to a cryptocurrency and their consensus protocols, such as proof-of-work (PoW). PoW consensus protocol was presented in [18] in the framework of the first application of blockchain technology for Bitcoin cryptocurrency management. PoW is based on so-called "mining": a process of looking for a nonce – a random number that is stored in every block – so that the resulting hash of a new valid block satisfies certain requirements. These requirements set the difficulty threshold for the process of finding the nonce and determines the average number of hashes needed to mine one block. This impacts the amount of energy to be spent to find such nonce. In 2013 the amount of energy used by Bitcoin mining was already comparable to the Irish national energy consumption [22]. Existing PoW blockchains can achieve throughput of not more than 60 transactions per second without significantly affecting the blockchain's security [23]. These findings show that PoW can negatively impact the system scalability and overall throughput [24]. Trying to address these issues researchers have challenged various aspects of the Bitcoin system and proposed modifications in its core operation, e.g., modification of the block generation rate or alternative proof of work implementations. A security analysis of PoW based consensus protocols can be found in [25].

A permissioned blockchain in contrast has means to identify the nodes that can control and update the shared state, and often also have ways to control who can issue transactions. Consensus protocols for reaching an agreement by exchanging messages even if some nodes fail, collude, or send the corrupted messages could be employed in permissioned blockchain systems. In [20] the authors present an overview of consensus protocols used in the context of permissioned blockchains. The authors also review the underlying principles, and compare the resilience and trustworthiness of some protocols as well as the permissioned

[5] Smart contract and chaincode logic concepts are quite close, therefore, we use the former when talking about programmable contract, or a set of rules, when discussing BCT in general.

blockchain systems (e.g., Hyperledger Fabric, Tendermint, R3 Corda, and MultiChain).

Another approach to constructing a blockchain relies on properties of Keyless Signatures Infrastructure (KSI) [26]. KSI is a globally distributed system for providing time-stamping and server-supported digital signature services. KSI blockchain (Guardtime) employs chain-resistance property of hash functions to verify the integrity of the data using hash-chain. KSI Blockchain deployed, for instance, in Estonian government networks to insure the integrity of the data stored in government repositories and protect them against insider threats. The number of participants in the KSI consensus protocol is limited, which allows to eliminate the need for PoW and ensuring that settlement can occur within one second. However, major drawbacks of such approach is limited decentralization and required trust in the participants of KSI consensus.

3 Review Methodology

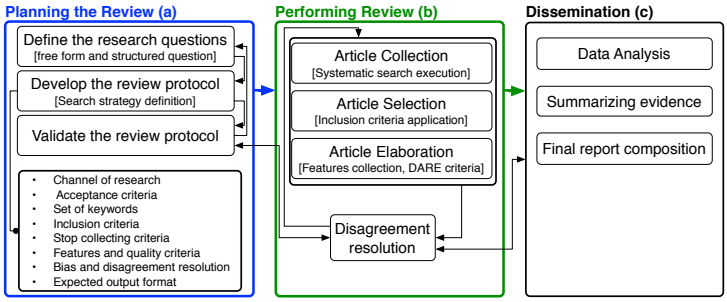

Fig. 1. Review Methodology Structure according to [27] and [28].

To provide a comprehensive study, we have opted for performing a systematic, rigorous and reproducible process of retrieval, selection, and analysis of relevant literature.This paper adheres to the procedure adopted and adapted by [29] (see Figure 1).

Following the Goal-Question-Metric (GQM) [30], the generic free-form question *"What challenges demand the employment of BCT in MAS, and is this employment justified?"* is broken-down in following *structured research questions* (SRQs).

SRQ1: *How has the combination of BCT in MAS evolved over the years in terms of* ***when*** *(year) and* ***where*** *(geographical indication of the scientific institute) such research took place?* **SRQ2:** *What are the motivations supporting the employment of blockchain in agent-based systems?* **SRQ3**: *What are the* ***application domains*** *and* ***scenarios*** *used to test or employ blockchain technologies? What are the* ***requirements*** *such approaches aimed at meeting?* **SRQ4:** *What are the* ***mechanisms*** *and related* ***assumptions*** *within the proposed protocols/approaches characterizing the most relevant contributions?* **SRQ5:** *What are the* ***strengths*** *and* ***limitations*** *that such technologies might imply?* **SRQ6:** *What are the* ***stated future research directions*** *and* ***challenges*** *identified by the scientific community?*

To perform a more accurate semi-automatic research, some keywords have been contextualized. Based on the reviewers' rooted backgrounds on MAS and BCT domains, following keywords were defined: *Blockchain + MAS, Blockchain + multi-agent system, Blockchain + smart contract + multi-agent system, smart contract + multi-agent system + trust*. The initial collection counted 36 papers. A further coarse-grained examination, processing the compliance of the selected abstracts with the following *inclusion criteria*, reduced them to 14.

A) **Context:** The primary studies should define their contributions in the context of blockchain technology employed in agent-based systems.
B) **Purpose:** The purpose of primary studies has to refer to applying BCT seeking for traceability, commitment, security, and trust in MAS mechanisms such as negotiation, coordination, collaboration, and competition.
C) **Theoretical foundation:** The primary studies should provide at least one of the following elements: [visionary formulation, theoretical definition, system design].
D) **Practical contribution:** The primary studies should provide at least one of the following elements: [practical implementation, tests, critical analysis, critical evaluations or discussion].

4 Results presentation

This section presents the outcomes obtained by performing the methodology presented in Section 3. We are following the research questions presented above.

Table 1. Domains and application scenarios.

Domain	Application	Ref.	Astr.
Collaborative governance	-transactive energy systems	[7]	T
	-conflicts resolution in business collaboration	[9]	C
	-legal accountability (regular and self-aware contracts)	[31]	P
	-task,allocation, coordination, and supervision of a group of people who share,common economic interests	[13]	C
Big data management	-management and collection of big data in highly distributed environment	[8]	C
	-anonymization of distributed data	[32]	T
Coordination	-distributed artificial intelligence	[10]	C
	-swarm robotics	[14]	C
	-coordination models in IoT	[33]	C
Trust, Data integrity, Reputation management	-reputation management in P2P clusters	[15]	T
	-formalisation of validation and authentication protocol for secure identity assurance	[34]	P
	-eCommerce, demand-supply relationships	[35]	P
	-supply and value chains in industrial environments and marketplaces	[36]	C
	-software life-cycle development	[37]	C

To answer **SQR1** we looked where and when the research presented in the selected papers has been conducted. Almost all the articles were published in 2017 (10 studies), while among them, one study [10] as well as another work from 2016 [14] were found on arXiv e-Print. In addition, one paper was published in 2015, and one is accepted to be presented on a congress that will take place in 2018 [37]. Due to the adoption of KSI blockchain technology in Estonia, a number of works (4 out of 14) were produced entirely or partially in Estonia.

Otherwise, researchers all over the world started exploring the possibilities of employing BCT in the area of MAS: one can find contributions form Europe, US, Japan, China, and Russia.

Concerning **SQR2**, we analyzed the *opportunities* and the *motivations* characterizing MAS and BCT with respect to existing technologies/approaches. The motivation for applying BCT in the framework of MAS was almost always based on the *requirements* determined by the application scenario for the multi-agent systems in question. We list the requirements with the corresponding applications when answering **SQR3** below. The need for accountability, transparency, and trust is of high importance in many applications of MAS. In [33], the authors, for instance, are seeking for establishing accountability, traceability, and transparency of interaction for tuple-based coordination. In [34,32,9,36] issues and challenges related to identification and trust are raised by the authors. Employing smart contracts, and having an access to the distributed ledger, in addition to addressing the issues just mentioned above, could also provide a simplified solution for a distributed master-less reputation management as stated in [15].

Addressing **SQR3**, we grouped selected works based on their *domains* (i.e. classification of the main purpose or usage of BCT), and listed the *application scenarios* explored. Table 1 presents the domains and the application scenarios, for which combination of MAS and BCT principles could be beneficial, as stated in the analyzed research works. For every paper, based on the maturity of the work, we specify the abstraction level: Conceptual (C), Prototype (P), or Tested (T). One could notice that more then 50% of the works are still at the conceptual level (C). Only three articles present system prototypes (P) and the three others provide evaluation of the proposed solutions.

The majority of the papers focus on collaborative governance and trust and reputation management. Among the applications, the following use-case scenarios are elaborated the most: an approach for energy trades in an open P2P market, while insuring anonymity and security of the participants [7]; a prototype of a system for blockchain-driven self-aware agents-assisted contracts [31], a distributed multi-level reputation scoring system implemented into P2P clusters [15]; trust management for both supply-demand relationships [35], and for the process of software verification [34]. In a more orthogonal position, [13] reveals a number of challenges, potential difficulties, and pitfalls that have to be considered when applying BCT.

Using blockchain technology for management of big distributed datasets and for coordination mechanisms between the agents were also proposed. The authors in [32], for instance, suggest to use BCT for keeping the log of all the transactions such as creation of privacy policy, data exchange, and data anonymization. Regarding the employment of BCT for agent coordination, only very preliminary results were found. These works just motivate the possibility to use BCT, or mention coupling MAS and BCT as a future research possibility. For instance, blockchain technology were proposed to be applied when multiple swarms from competitor companies have to coexist in the same environment, such as in mining scenarios, intelligent transportation environments, or search and rescue missions [14]. The authors in [10] try to address the drawback of existing Artificial

Intelligence (AI) systems that are managed by a central server (thus, distributed, but not decentralized). Therefore, these systems are limited in performing complex organization and planning, and in solving composite tasks. The authors propose to use BCT for decentralization of AI. This would allow to solve problems with virtually unlimited power and maximum efficiency [10]. According to [33], BCT could be used to bring accountability, traceability, and transparency of interactions, and to strengthen suitability of applying the tuple-based coordination models (such as TuCSoN [38]), in different domains, such as healthcare, or IoT.

To answer **SQR4** we list the *mechanisms* and related *assumptions* characterizing the existing solutions. We focus on the papers that present solutions that were prototyped or already tested. For the transactive energy system proposed in [7] Kvaternik et al. employ a decentralized computation fabric based on Ethereum, a novel trading sequence implementation (including fulfillment of partial trades), as well as off-blockchain communications. Kiyomoto et al. [15], in the framework of multi-level scoring systems for P2P clusters, employ BigchainDB [39] -– a technology that combines the properties of decentralized processing platforms like Ethereum, and decentralized file systems like InterPlanetary File System (IPFS). The authors assume that in the MAS the agents are not trusted i.e., each node can play his own game. Private BCT, Hyperledger v0.6 is used in [32] for trading anonymized datasets. ADI (anima-desire-intention) model with 6 dimensions (physiology, belief, character, knowledge, experience, and context) are employed in [35] to model interactions of supply-demand information agents.

Next question, **SQR5**, concerns the advantages of the research work presented in the selected papers. We first summarize the strengths and then list the limitations that were identified by the authors. It is broadly acknowledged that BCT enables business collaborations that require high-reliability and shared, trusted, privacy-preserving, immutable data repositories, and smart contracts execution [40]. Moreover, coupling BCT-based smart contracts with MAS opens the door to new interesting scenarios, such as simplifying the distributed governance of groups of people [13]. By doing so, transaction costs for reaching an agreement can be reduced, fostering the formalization and enforcing relationships between people, institutions, and the assets they own, by standardizing transaction rules [13]. MAS dynamics are a very close representation of human society, therefore, tracking their interactions while guaranteeing their immutability can prevent situations where two or more parties claim the opposite about whether a payment or a service has been performed. Moreover, besides immutability of values, this entails that events are immutable over time (timestamped).

The language for executing self-aware contracts (SAC) proposed in [31] is based on obligations and a more static and declarative approach. However, the relation between declarative and imperative programming in smart contracts is still an open challenge. Thus, whether logic (e.g., voting protocols/algorithms) can also be covert in this way is another interrogative. Nevertheless, there is still a lack of a framework supporting migration from a smart- towards a self-aware contract. The latter has the ability to gather information about their

internal/external-contextual state and progress to reason about their behavior while being a law artifact [31]. Immutability implies storing (machine-readable and agent-executable) the contract and its obligations, which to this extent, might increase the complexity. [7] also mentions one limitation related to Solidity[6] a language for creating smart contracts on the Ethereum platform.

We finally focus on **SQR6** and summarize future challenges. As the majority of the papers present the work at the conceptual level, implementation of the proposed scenarios was stated as a future challenge by the authors in [8,14,33,34,36,10,37]. More mature solutions, for instance, [7], identify the need to improve anonymity of the nodes, in case of employing public blockchain implementation such as Ethereum. Taking into account the risks of de-identification, due to the possibility to track and link the transactions of a user [41,42], the authors in [7] suggest some countermeasures, such as onion routing [43], or employing a large number of anonymous addresses. However, in practice, these countermeasures do no guarantee that de-identification of a user is not possible. Another work [15] indicates the need to perform large-scale evaluation and the need to achieve scalability of their distributed multi-level reputation scoring system. Developing economical models and defining optimal settings for the platform, as proposed in [32] for datasets trading, was also listed as a future challenge.

5 Discussion

When a new technology is unveiled or it makes a brake-through in new application domains, many questions arise, especially concerning when and how to apply it depending on requirements and context. The emergence of BCT and its integration in agent-based systems requires a better comprehension of the implications and the impact of this new technology, as we have seen in the research works analyzed in this paper. Hence, in this section we first aim at understanding whether combining BCT and MAS is justified, or if alternative approaches might be employed. Then, after discussing about current solutions and our vision, we identify the main open challenges in the field.

Justification of binding MAS and BCT Papers providing mostly conceptual contributions discuss the potential benefits of combining BCT and MAS. However, no in-depth analysis, demonstration, or concrete evaluation of its necessity are provided. For example, the authors in [8], suggest using MAS to solve the scalability issues, common in most blockchain architectures. Nevertheless, no further details are provided on how this could be concretely achieved. Moreover, in [9], the authors present smart contracts developed for cross-organizational collaboration. Then, it is only mentioned as a future direction the possibility of exploring how blockchain technology can realize non-repudiation in process-aware smart contracting governance. Given that many of these works are still on a preliminary stage, it is the case that several key aspects such as the ones above-mentioned are still undeveloped.

[6] https://solidity.readthedocs.io/en/develop/

Correctness in applying BCT in the framework of MAS Concerning the findings provided by concrete solutions, the necessity of such contribution is often questionable, and therefore it might be that the employment of BCT is also questionable. For example, the authors of [32] propose to use private blockchain as a "service" to keep track of the agreements provided by owners of data and transactions containing information about sharing anonymized data-sets, in order to allow the data owners to track all the events of the data sharing process. While keeping an immutable log containing all the user agreements is very important, it does not fully justify the use of private blockchain technology. According to the existing laws on the area of management of information about individuals (including sensitive data)[7], once the data are properly anonymized such that de-identification is not possible by any reasonable means, these data do not belong to the initial data owner anymore. Thus, keeping the log about all the transactions, as well as participating in the consensus protocol (especially for the data clients that do not need to access multiple data-sets) may be a burden and will not contribute to the usability or adoption of the system.

Furthermore, it is worth to focus on the correctness of the BCT application in a given problem or scenario. However, it is challenging to justify the correctness of the solutions that are still at the conceptual stage. Nevertheless, some of the selected primary studies, describing more developed solutions, list as well their argumentation supported by the presented evaluation results [7,15]. For instance, in [32], the authors mention that one of the benefits of their approach is that no central server managed by a trusted third party (TTP) is required, therefore the cost of deployment of such system can be reduced as there is no need to maintain the TTP. However, the solution in [32] uses Hyperledger Fabric – implementation of the private blockchain technology – and therefore, requires membership service, as well as certification authority for registering users and distributing the credentials (public/private keys).

Open challenges of BCT towards MAS application scenarios Even in cases where the use of BCT was justified and correctly employed, several challenges still need to be addressed (the following analysis extends the one provided in [13]): *(i)* Creating a legal base for BCT; *(ii)* Verifying correctness of the chaincode/smart contracts; *(iii)* Preserving the distributed nature of BCT, by preventing creation of mining pools, and collusion among the nodes in the framework of public BCT; *(iv)* Developing solutions to ensure privacy and anonymity where appropriate; *(v)* Ensuring adoption of the new blockchain technology; *(vi)* Managing membership service in the framework of permissionned BCT; *(vii)* Addressing scalability issues of BCT; *(viii)* Ensuring reliability of the mechanisms on which BCT is built and are often used in combination with e.g., key management, hashing, digital signature, encryption. Although some of these challenges are also present outside MAS scenarios, addressing appropriately will have a deep impact on the adoption of BCT in agent-based systems

[7] EC Data Protection Directive 95/46/EC; Health Insurance Portability and Accountability Act.

It is also highly important to evaluate whether the MAS requirements for every application scenario could be addressed without BCT. The authors in [44] provide a diagram that could be used to help to evaluate whether the use of BCT is justified. One has to take into account that given that this technology is still being developed, there is a number of issues that may affect early adopters. These include the lack of scalability of the current implementations of BCT, as well as the complexity of the blockchain technology, which could be more substantial then the benefits brought when applying it. Choosing the technology implementation (public/private BCT), defining what kind of data should be stored on-, and off-blockchain are essential questions. In the majority of the papers selected for the review, these points were not adequately addressed. Table 2 shows how the properties of BCT can fulfill multiple MAS requirements.

Table 2. Mapping between MAS requirements and the main properties of the BCT.

		BCT properties				
		Immutability	Complete History	Distributed Consensus	Cryptography primitives (e.g., hash, digit sign)	Smart Contract
MAS requirements	Trust	X	X	X	X	X
	Reputation	X	X	X		
	Data integrity	X	X	X	X	
	Traciability	X	X	X		X
	Transparency	X	X	X	X	X
	Anonymity				X*	
	Privacy	X			X*	
	Authenticity	X	X	X	X	

According to the evidence elaborated in this study, reputation, transparency, and traceability are crucial in case of competitive behavior among the agents, whereas trust and accountability are of a high importance for collaborative behavior.

Unfortunately, not all the features of MAS requiring support could gain advantages by applying BCT to MAS. However, Table 2 proposes a possible mapping elicited by studying current solutions or the proposed designs. For instance, the authors in [9] propose to investigate how BCT could be used to address privacy issues, yet, blockchain solely does not provide a general solution for privacy and anonymity [41,42]. However, BCT could be used for ensuring/enforcing role-based access control, or privacy-policy management [33,32,45]. To address the anonymity and privacy requirements, additional mechanisms have to be employed, e.g., crypthographic primitives used off-blockchain (hence, marked with the * in the Table 2), secret sharing scheme [46], secured multi-party computations [47] as proposed in [48], communication anonymity solution, such as onion routing, as mentioned in [7]. However, the scalability limitations of BCT, especially in case of using private blockchain technology, can create a barrier when applying BCT.

Employing MAS and BCT in real-world applications Hereafter, we present our vision regarding potential applications where coupling BCT and MAS could be highly beneficial. For instance, in the healthcare domain, and particularly in connected health, the following scenario could be considered. Every actor (e.g., caregiver, insurance, pharmacy, healthcare / ambient assisted living device) can be modeled as an agent with a different behavior. Some agents could

be cooperative and trusted (e.g., caregiver and pharmacy), and the others may require reputation management, and transparency in order to ensure correct behavior. Such MAS would benefit from all main properties of the blockchain: immutability, traceability, distributed consensus, use of cryptographic primitives, and ability to define functionality of the system using smart contracts. Smart contracts could be used for managing insurance claims, reimbursements of the medications, payments of medical visits, privacy policy management. Designing emergency access to the data could be based on the BCT and deployed using witness *cothority* [49]: a "collective authority" whose purpose is to witness, validate, and cosign the statements.

Moreover, BCT can be employed for data sharing, and evaluating an anonymity level of individuals given access control policy, and shared data. This approach may bear similarities with [32], yet it has an important conceptual difference: not only to track the datasets that contain the data owner information [32], but rather maintain what kind of information were exactly shared, and use this to adjust the anonymization process for the consequent data releases, or updates. Employing BCT in different healthcare scenarios has already been proposed in [50,51,52], and several prototypes exist [53,45]. Principles of MAS are as well often applied in healthcare domain [28,54,55]. Possibility to combine MAS and BCT to improve healthcare management has already been mentioned in [33].

MAS can be as well successfully combined with BCT in information systems for supporting business-to-business (B2B) electronic commerce, where software agents represent different companies involved in B2B e-commerce [56]. Until now, distributed systems of this kind have required a trusted mediator that stores the transactions occurring between the parties, such as ordering, supplying, and paying. As has been argued in [34], BCT enables to get rid of the role of such a mediator by storing transactions in a distributed ledger based on BCT. Moreover, in addition to transactions, also commitments and meta-commitments can be securely stored in a distributed ledger.

Another area where the combination of MAS and BCT can be useful is societal information systems [57] that gather information from hundreds of nodes, each associated with a person. Recently, such systems became known as platforms for sharing economy, such as Uber and AirBnB. These platforms usually have a central mediator that processes the information at its disposal in its own interests and only selectively shares it between the participants. Systems of this kind can be "democratized" so that they would better reflect the spirit of sharing economy by representing each node in a network by a software agent.

6 Conclusions

This paper proposed an SLR applied to 14 primary studies supporting the adoption of BCT in MAS. An overview of their domains, requirements of the application scenarios, motivations, assumptions, strengths, limitations, and identified future challenges has been provided. We also discussed correctness and justification of using BCT to address the requirements of MAS. We then proposed our vision on how MAS and BCT could be combined in different application scenar-

ios. Ongoing work focuses on addressing open challenges of employing blockchain technology in the framework of MAS, formalizing them in a roadmap. Future work includes the implementation of the conceptual solutions that propose adequate applications of BCT in MAS.

References

1. Schatten, M., Ševa, J., Tomičić, I.: A roadmap for scalable agent organizations in the internet of everything. Journal of Systems and Software **115** (2016) 31–41
2. Calvaresi, D., Sernani, P., Marinoni, M., Claudi, A., Balsini, A., Dragoni, A.F., Buttazzo, G.: A framework based on real-time os and multi-agents for intelligent autonomous robot competitions. In: IEEE Symposium on Industrial Embedded Systems (SIES). (2016) 1–10
3. Calvaresi, D., Marinoni, M., Sturm, A., Schumacher, M., Buttazzo, G.: The challenge of real-time multi-agent systems for enabling iot and cps. IEEE/WIC/ACM International Conference on Web Intelligence (2017)
4. Yu, B., Singh, M.P.: An evidential model of distributed reputation management. In: Proceedings of the first international joint conference on Autonomous Agents and Multiagent Systems: Part 1, ACM (2002) 294–301
5. RAMCHURN, S.D., HUYNH, D., JENNINGS, N.R.: Trust in multi-agent systems. The Knowledge Engineering Review **19**(1) (2004) 1–25
6. Hedin, Y., Moradian, E.: Security in multi-agent systems. Procedia Computer Science **60** (2015) 1604 – 1612 Knowledge-Based and Intelligent Information and Engineering Systems 19th Annual Conference, KES-2015, Singapore, September 2015 Proceedings.
7. Kvaternik, K., Laszka, A., Walker, M., Schmidt, D., Sturm, M., Dubey, A., et al.: Privacy-preserving platform for transactive energy systems. arXiv preprint arXiv:1709.09597 (2017)
8. Qayumi, K.: Multi-agent based intelligence generation from very large datasets. In: Cloud Engineering (IC2E), 2015 IEEE International Conference on, IEEE (2015) 502–504
9. Norta, A., Othman, A.B., Taveter, K.: Conflict-resolution lifecycles for governed decentralized autonomous organization collaboration. In: EGOSE. (2015) 244–257
10. Ponomarev, S., Voronkov, A.: Multi-agent systems and decentralized artificial superintelligence. arXiv preprint arXiv:1702.08529 (2017)
11. Swan, M.: Blockchain: Blueprint for a new economy. (2015)
12. Tapscott, D., Tapscott, A.: Blockchain Revolution: How the technology behind Bitcoin is changing money, business, and the world. Penguin (2016)
13. Shermin, V.: Disrupting governance with blockchains and smart contracts. Strategic Change **26**(5) (2017) 499–509
14. Ferrer, E.C.: The blockchain: a new framework for robotic swarm systems. arXiv preprint arXiv:1608.00695 (2016)
15. Gattermayer, J., Tvrdik, P.: Blockchain-based multi-level scoring system for p2p clusters. In: Int Conf Parallel Processing Workshops ICPPW, IEEE (2017) 301–308
16. Russell, S.J., Norving, P.: Norvig. Artificial Intelligence: A Modern Approach (2003) 111–114
17. Ramchurn, S.D., Huynh, D., Jennings, N.R.: Trust in multi-agent systems. The Knowledge Engineering Review **19**(1) (2004) 1–25
18. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2008)

19. Pass, R., Shi, E.: Hybrid consensus: Efficient consensus in the permissionless model. In: LIPIcs-Leibniz International Proceedings in Informatics. Volume 91., Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik (2017)
20. Cachin, C., Vukolić, M.: Blockchains consensus protocols in the wild. arXiv preprint arXiv:1707.01873 (2017)
21. Buterin, V.: Ethereum: A next-generation smart contract and decentralized application platform. URL https://github. com/ethereum/wiki/wiki/% 5BEnglish% 5D-White-Paper (2014)
22. O'Dwyer, K.J., Malone, D.: Bitcoin mining and its energy footprint. In: ISSC 2014/CIICT 2014, IET (2013) 280–285
23. Gervais, A., Karame, G.O., Wüst, K., Glykantzis, V., Ritzdorf, H., Capkun, S.: On the security and performance of proof of work blockchains. (2016) 3–16
24. Vukolić, M.: The quest for scalable blockchain fabric: Proof-of-work vs. bft replication. In: International Workshop on Open Problems in Network Security. (2015)
25. Kiayias, A., Panagiotakos, G.: On trees, chains and fast transactions in the blockchain. IACR Cryptology ePrint Archive (2016)
26. Buldas, A., Kroonmaa, A., Laanoja, R.: Keyless signatures' infrastructure: How to build global distributed hash-trees. In: Nordic Conference on Secure IT Systems. (2013) 313–320
27. Kitchenham, B., Pearl Brereton, O., Budgen, D., Turner, M., Bailey, J., Linkman, S.: Systematic literature reviews in software engineering - a systematic literature review. Information and Software Technology **51**(1) (2009) 7–15
28. Calvaresi, D., Cesarini, D., Sernani, P., Marinoni, M., Dragoni, A., Sturm, A.: Exploring the ambient assisted living domain: a systematic review. Journal of Ambient Intelligence and Humanized Computing (2016) 1–19
29. Calvaresi, D., Appoggetti, K., Lustrissimini, L., Marinoni, M., Sernani, P., Dragoni, A.F., Schumacher, M.: Multi-agent systems' negotiation protocols for cyber-physical systems: Results from a systematic literature review. In: Proceedings of ICAART. (2018)
30. Kitchenham, B., Brereton, P., Turner, M., Niazi, M., Linkman, S., Pretorius, R., Budgen, D.: Refining the systematic literature review process-two participant-observer case studies. Empirical Software Engineering **15**(6) (2010) 618–653
31. Norta, A., Vedeshin, A., Rand, H., Tobies, S., Rull, A., Poola, M., Rull, T.: Self-aware agent-supported contract management on blockchains for legal accountability. White paper (2017)
32. Kiyomoto, S., Rahman, M.S., Basu, A.: On blockchain-based anonymized dataset distribution platform. In: Software Engineering Research, Management and Applications (SERA), 2017 IEEE 15th International Conference on, IEEE (2017) 85–92
33. Mariani, S., Omicini, A., Ciatto, G.: Novel opportunities for tuple-based coordination: Xpath, the blockchain, & stream processing
34. Leiding, B., Norta, A.: Mapping requirements specifications into a formalized blockchain-enabled authentication protocol for secured personal identity assurance
35. Shen, J., Shen, J., Huang, Y., Huang, Y., Chai, Y., Chai, Y.: A cyber-anima-based model of material conscious information network. Int J of Crowd Science (2017)
36. Bonino, D., Vergori, P.: Agent marketplaces and deep learning in enterprises: The composition project. In: Annual Computer Software and Applications Conference. (2017) 749–754
37. Fuller, T.R., Deane, G.E.: Anomaly detection and intelligent notification. In: Future of Information and Communications Conference. (2018)
38. Omicini, A., Zambonelli, F.: Coordination for internet application development. Autonomous Agents and Multi-Agent Systems **2**(3) (Sep 1999) 251–269

39. McConaghy, T., Marques, R., Müller, A., De Jonghe, D., McConaghy, T., McMullen, G., Henderson, R., Bellemare, S., Granzotto, A.: Bigchaindb: a scalable blockchain database. white paper, BigChainDB (2016)
40. Hull, R., Batra, V.S., Chen, Y.M., Deutsch, A., Heath III, F.F.T., Vianu, V.: Towards a shared ledger business collaboration language based on data-aware processes. In: International Conference on Service-Oriented Computing, Springer (2016) 18–36
41. Androulaki, E., Karame, G.O., Roeschlin, M., Scherer, T., Capkun, S.: Evaluating user privacy in bitcoin. In: Intl Conference on Financial Cryptography and Data Security. (2013)
42. Möser, M.: Anonymity of bitcoin transactions. In: Münster bitcoin conference. (2013) 17–18
43. Dingledine, R., Mathewson, N., Syverson, P.: Tor: The second-generation onion router. Technical report, Naval Research Lab Washington DC (2004)
44. Wüst, K., Gervais, A.: Do you need a blockchain? IACR Cryptology ePrint Archive (2017)
45. Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., Wang, F.: Secure and trustable electronic medical records sharing using blockchain. arXiv preprint arXiv:1709.06528 (2017)
46. Shamir, A.: How to share a secret. Commun. ACM (11) (November 1979) 612–613
47. Ben-Or, M., Goldwasser, S., Wigderson, A.: Completeness theorems for non-cryptographic fault-tolerant distributed computation. In: ACM symposium on Theory of computing. (1988)
48. Zyskind, G., Nathan, O., et al.: Decentralizing privacy: Using blockchain to protect personal data. In: Security and Privacy Workshops. (2015)
49. Syta, E., Tamas, I., Visher, D., Wolinsky, D.I., Jovanovic, P., Gasser, L., Gailly, N., Khoffi, I., Ford, B.: Keeping authorities "honest or bust" with decentralized witness cosigning. In: Symposium on Security and Privacy. (May 2016) 526–545
50. Kuo, T.T., Kim, H.E., Ohno-Machado, L.: Blockchain distributed ledger technologies for biomedical and health care applications. J American Medical Informatics Assoc **24**(6) (2017)
51. Yue, X., Wang, H., Jin, D., Li, M., Jiang, W.: Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. Journal of medical systems (2016)
52. Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., Wang, F.: How blockchain could empower ehealth: An application for radiation oncology. In: VLDB Workshop on Data Management and Analytics for Medicine and Healthcare, Springer (2017)
53. Ekblaw, A., Azaria, A., Halamka, J.D., Lippman, A.: A case study for blockchain in healthcare“medrec” prototype for electronic health records and medical research data. (2016)
54. Calvaresi, D., Schumacher, M., Marinoni, M., Hilfiker, R., Dragoni, A., Buttazzo, G.: Agent-based systems for telerehabilitation: strengths, limitations and future challenges. In: Proc. of X Workshop on Agents Applied in Health Care. (2017)
55. Dubovitskaya, A., Urovi, V., Barba, I., Aberer, K., Schumacher, M.I.: A multiagent system for dynamic data aggregation in medical research. BioMed Research International (2016)
56. Taveter, K.: Agile engineering of b2b automation systems. ERCIM News (2004)
57. Taveter, K., Du, H., Huhns, M.N.: Engineering societal information systems by agent-oriented modeling. J of Ambient Intelligence and Smart Environments **4**(3) (2012) 227–252