Journal of Network and Computer Applications 170 (2020) 102814

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Smart contracts for blockchain-based reputation systems: A systematic literature review

Ahmed S. Almasoud [a,b,*], Farookh Khadeer Hussain [a], Omar K. Hussain [c]

[a] School of Software, University of Technology, Sydney, NSW, Australia
[b] College of Computer and Information Sciences, Prince Sultan University, Riyadh, Saudi Arabia
[c] School of Business, University of New South Wales, Canberra, ACT, Australia

ARTICLE INFO

Keywords:
Blockchain
Ethereum
Reputation systems
Smart contracts

ABSTRACT

Reputation systems offer a medium where users can quantify the trustworthiness or reliability of individuals providing online services or products. In the past, researchers have used blockchain technology for reputation systems. Smart contracts are computer protocols which have the primary objective to supervise, implement, or validate performances or negotiations of contracts. However, through a systematic literature review, in this paper, we find that the existing literature has not proposed a framework that facilitates the interchangeable use of smart contracts for blockchain-based reputation systems. We adopt a systematic literature review from 30 relevant studies and the data from them were extracted before identifying the research gaps. As a solution to the research gaps, we propose the FarMed framework for creating an intelligent framework that will execute Ethereum smart contact-based reputation systems and develop reliable blockchain-based protocols for transferring reputation values from one provider to another. We briefly explain our proposed framework before concluding with our future work.

1. Introduction

In a distributed decentralized environment, establishing an online presence is simple and easy but it provides little evidence about the trustworthiness of an individual. Thus, when service provisioning occurs between entities who have, hitherto, not made transactions with each other, the notion of trust and/or reputation is used to ensure that the service requestor accepts the risk of transacting with the service provider even before it receives the service (Audun et al., 2007). Reputation systems provide a platform through which such users can measure the legitimacy of people offering online services or products (Casassa et al., 2001). Typically, reputation systems allow a service requestor to rate an individual's (service provider's) ability to provide online services and the (aggregated or cumulated) score of the service provider can be used by other individuals to decide whether they want to transact with the said individual.

Over the years, reputation systems have been widely implemented in various industries such as e-commerce applications (Christidis, 2018), the financial services industry etc. In these areas, various advancements using reputation systems as their base have been made to facilitate the processes. For example, in e-commerce, various companies such as eBay, Amazon, Alibaba, Shopify, Magento, Wix, OpenCart, and SquareSpace use reputation systems to underpin technologies such as mobile commerce, digital funds transfers, electronic data interchange (EDI) etc. In financial systems, reputation systems play a pivotal role too in helping financial institutions build their reputation over time and boost the viability of their operations. However, in all these cases, the reputational information is stored in either a decentralized or centralized way. While storing the information in a centralized manner has advantages to the user(s) who wish to retrieve the data whenever they need it, it also has several challenges such as denial-of-service (DoS) attacks which render such a system completely ineffective. These drawbacks can be addressed by storing the information in a decentralized way where the reputation values are stored across multiple nodes. In such an environment, users can retrieve ratings (for the provider) from other users in a distributed manner and make decisions. But this platform has its own drawbacks in relation to security issues, such as rating fraud and rating manipulation. These drawbacks render the reputation systems useless as they are not able to support many users, ensure the integrity of the ratings or trust scores, and also provide reliable mechanisms to support new users to bootstrap into the reputation-based economy.

The advent of blockchain technologies is a means to address these

* Corresponding author. University of Technology, Sydney, Australia.
E-mail addresses: Ahmed.Almasoud@student.uts.edu.au (A.S. Almasoud), o.hussain@adfa.edu.au (O.K. Hussain).

https://doi.org/10.1016/j.jnca.2020.102814
Received 10 September 2019; Received in revised form 14 May 2020; Accepted 12 August 2020
Available online 23 August 2020

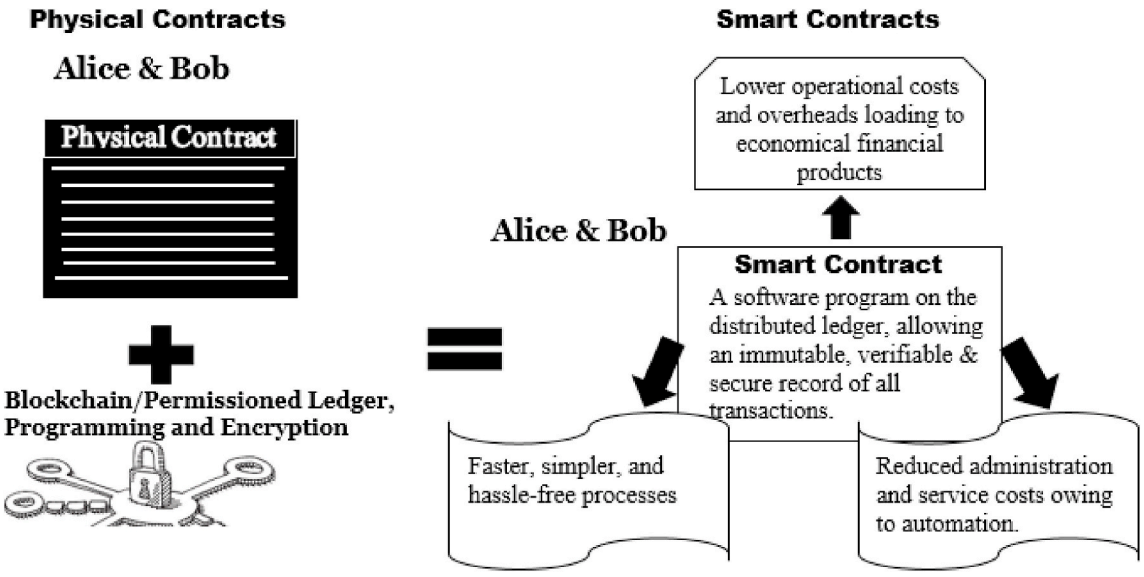

Fig. 1. Relationship between smart contract and blockchain technology.

drawbacks. As noted by Sherman (2018), blockchain is a way to change how online reputation systems are managed. By integrating a proof-of-individuality framework in the verification system, a blockchain model guards against Sybil attacks and prevents scenarios such as forgery, creation of multiple identities, manipulating scores etc. This technology has led researchers to make new advancements to further carry out processing efficiently. One such advancement is the development and implementation of smart contracts. Smart contracts are software codes that run over the blockchain technology to implement the different required transactions. As shown in Fig. 1, they are akin to traditional contracts, but have the capabilities of being self-enforcing, far more efficient, and less onerous on the seller and buyer (Toneli et al., 2018).

However, as it is with any new technology, there are several open research issues that exist in the wide implementation of smart contracts. The objective of this paper is to understand such current issues by performing a systematic literature review (SLR), which in the topic of the study performs a categorical analysis of the literature (Petticrew and Roberts, 2006). The categorical analysis is undertaken in the five broad areas in which smart contracts and blockchain-based reputation systems have limitations. These are the inability of service users in (1) deriving the reputation value of service providers based on the values (or ratings) present in the smart contracts; (2) predicting the future trust value of a service provider based its trust values in the blocks; (3) considering the reputation of a service provider as a digital asset and moving across platforms; (4) detecting and dealing with reputation fraud such as bad mouthing, ballot stuffing, positive and negative discrimination, false feedback, and the value imbalance problem etc; and (5) mathematical models and algorithms that assist in addressing the abovementioned gaps. The need to address these drawbacks will be explained in the next section before performing an SLR to enrich smart contracts in these areas.

The structure of the paper is as follows. Section 2 presents five key requirements that should serve as the pillars of a smart contract-based reputation system. In section 3, the adopted process of shortlisting the papers chosen for this SLR is discussed. This includes discussing the criteria for searching the literature as well as the inclusion and exclusion criteria. Section 4 presents a summary of all the papers that have been shortlisted, totaling 30 in all. In section 5, a framework named FarMed Service is proposed as a smart contract-based reputation system service and all its components are thoroughly discussed. Finally, section 6 concludes the SLR and sets the stage for future research work.

2. Key requirements from a smart contract

This section discusses factors to be considered in smart contracts that

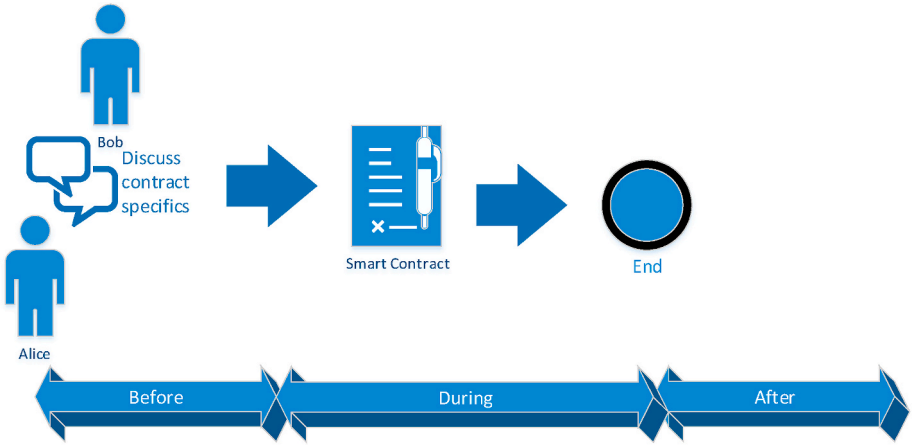

Fig. 2. The three phases of a smart contract.

will form the basis of a comparison of different existing papers in this SLR. Smart contracts are computer protocols designed to oversee, enforce, or verify performances or negotiations of contracts (Delmolino et al., 2016). By ensuring that no third parties are present during the processing of such transactions, which are irreversible and leave a trail of records for record-keeping, these protocols ensure their credibility (Buterin, 2017). These characteristics are beneficial and assist the user in the *during* phase of the smart contract. As shown in Fig. 2, the smart contract phase between Alice (user) and Bob can be categorized into three different phases, namely *before*, *during* and *after*. Before is that phase in which Alice and Bob negotiate to decide on the specifics of the smart contract, prior to forming it. During is the phase of collaboration governed by the smart contract, while after is the phase from the expiration of the smart contract.

For the wide application of smart contracts, apart from focusing on the during phase, users like Alice need certain requirements too, as follows:

2.1. Ability to derive overall reputation value of service providers based on the values (or ratings) present in the smart contracts (hereafter considered as Req: 1)

Smart contracts allow transactions to be stored and documented in a ledger that is distributed and shared between multiple parties (also known as nodes) hence there is no possibility of the loss of a ledger. While they guarantee the truthfulness of operations in the *during* phase, they do not assist Alice in the *before* and *after* phases in tasks such as determining Bob's credibility to complete the required tasks. However, this is necessary as reputation systems provide users with the ability to share their experience with other users ensuring that such users have the ability to make sound decisions based on the feedback provided by individuals who have used the products or services (Khaqqi et al., 2018). From a service provider's point of view, having such information is necessary as this represents a marketing tool (Josang, 2009). Without this, Alice does not have a comprehensive framework to determine either with whom to form a contract and why or whether to form a contract with Bob or not?

2.2. Ability to determine the trust value of a service provider in a context (hereafter considered as Req: 2)

According to Atzori (2016), the reputation of a specific user has a narrow link with the trustworthiness of that user. Reputation can be defined as what is said about a user (by others); what is believed about the said user; or their character or stance. As a result, reputation is derived from the observations of all the members of a social network. A model is required to determine the reputation value of the service provider in a particular context. This will help in inferring Bob's credibility and modelling his reputation in a specific context thereby assisting Alice in making a decision.

2.3. Reputation system as a digital asset and moving across platforms (hereafter considered as Req: 3)

In most reputation systems, service providers like Bob start off with a neutral or zero ratings and have issues interacting with other users in the system due to their low or non-existent credibility. It becomes a difficult task for new entrants to provide their services to the market. However, as a reputation value is context specific, such providers may have expertise in other contexts which can be used by then as leverage in this context. The challenge is how can they use this so that their reputation value is not glued to a platform, instead, it will be platform agnostic with appropriate weightings. In other words, a service provider should has the opportunity to transfer reputation from one platform to another, thereby ensuring that the reputation they have earned is not lost and can be used for reputation exchange and bootstrapping of new users (Caesar, 2018).

2.4. Detection of non-compliant behavior (hereafter considered as Req: 4)

Sometimes, users may try to defeat the system by engaging in reputation fraud in smart contracts such as bad mouthing, ballot stuffing, positive and negative discrimination, false feedback, value imbalance problem etc. This can occur when a user provides ratings even when it has not transacted with a certain user thereby either giving an unfair advantage or hurting them in the process. This can also occur in cases where a service provider develops pseudonyms which they then use to rate themselves. The feedback can also be biased, which may hamper the effectiveness of a feedback-based reputation system (Tadelis, 2016). To avoid such instances, a smart contract should have validated methods of detecting and dealing with any reputation fraud it encounters.

2.5. Mathematical models and algorithms (hereafter considered as Req: 5)

In order to compute the current trust value of service provider/s by addressing the above-mentioned requirements, specific mathematical models and algorithms are required. Such models need to be intelligent and should have the ability to automatically aggregate the ratings of a service provider and derive its reputation value from its overall rating. The algorithm or model should also be linked to the electronic marketplace (network) and should store specific parameters such as the service provider's address, service consumer's address, rating, and timestamp in a blockchain. This is important as since records on blockchain are immutable, it means the ratings and reputation values can never be altered.

Josang et al. (2007) noted that there are different measures of computing reputation and trust values. These models range from using different measures such as the use of simple summation or average of ratings; Bayesian model, which takes binary ratings as input and compute reputation values by a statistical update of beta probability density functions; belief model, which is related to the probability theory but the sum of probabilities here do not necessarily add up to 1 as the remaining probability is regarded as uncertainty; fuzzy models, which use linguistics to represent to what degree a service provider can be described e.g. trustworthy or not trustworthy; and flow models, which use transitive iteration through looped or arbitrarily long chains to compute reputation values. The issue to be addressed here is what specific measure or a combination of measures to use according to the objective to be achieved for a smart contract-based reputation system.

These five factors form the basis of our investigation into the existing approaches in the literature to determine if they provide a solution to address the issues in the area of smart contracts. Therefore, questions about whether the existing methods assist in addressing these issues will be answered in the comparison. The next section details the approach used to shortlist the papers that are reviewed in the SLR.

3. Process adopted for shortlisting the papers for SLR

This section details on the process adopted to identify the relevant papers to be reviewed in the SLR. We adopted a four-step process:

Step 1: Searching the literature →This step involves defining the search terms, identifying the data sources and the process of data collection.
Step 2: Inclusion and exclusion criteria → Certain criteria are defined to guide the extraction of the most relevant studies.
Step 3: Quality Evaluation → Each of the articles or journal papers are reviewed based on two quality evaluation criteria.
Step 4: Data Analysis → After reviewing the selected studies, data is extracted and recorded.

Table 1
Summary of stages of evaluating and selecting relevant papers for SLR.

Evaluation Stage	Method	Assessment Criteria
1st	Identify the related studies from the databases	Include the search terms
2nd	Eliminate studies based on date of publication	Exclude studies published before 2013
3rd	Eliminate studies based on title	If title includes the search terms (i.e. "smart contracts in blockchain", "blockchain and reputation systems" or "smart contracts for blockchain reputation systems"), include in the study; otherwise, exclude
4th	Eliminate studies based on abstract	If abstract shows study is relevant, include it; otherwise, exclude

3.1. Step 1: criteria for searching the literature

This step involves deciding the following:

- Databases used: The electronic scientific databases and data sources selected to source the papers from for the SLR are as follows:
  1 Elsevier ScienceDirect (www.sciencedirect.com/)
  2 IEEE Xplore (www.ieexplore.ieee.org/Xplore/)
  3 Google Scholar (www.scholar.google.com.au/)

These databases were selected primarily because they provide enough coverage of the literature that is relevant for this SLR.

- Search terms used: In order to create records for building the literature database, the search terms "smart contracts in blockchain", "blockchain and reputation systems" and "smart contracts for blockchain reputation systems" were entered into the publication databases. This resulted in the retrieval of 122 papers from 18 publication venues. All the sources selected are those that include literature surveys or empirical studies.
- Required information from the selected papers: The specific information required for each record is the abstract and the full text document.
- Publication time of the records: For a paper to be considered for SLR analysis, it needed to be published after 2013. This is logical as there is very little consideration of the use of smart contracts and blockchain before this time period.

122 studies were found after searching the publication venues in this step. Of these, some papers were eliminated based on their publication date which reduced the number of papers to 109. The remaining publications were subject to further inclusion and exclusion criteria as mentioned in the next step.

3.2. Step 2: inclusion and exclusion criteria

Not all the records identified in the previous step are considered in the SLR. They are further shortlisted according to the following inclusion and exclusion criteria:

Inclusion criteria:

1. Must contain meta-analyses.
2. Present literature reviews and surveys with a defined search process, research question and data extraction. Regardless as to whether the literature review is only a part of the article or the main component, these articles are included.
3. All research works should be related to the study area.

Exclusion criteria:

Table 2
Papers that met the quality evaluation criteria from Step 3 of the selection process.

Study number	Date	Topic	Category
S1	2017	SCPKI: a smart contract-based PKI and identity system	Smart Contract
S2	2016	A decentralized sharing app running a smart contract on the Ethereum blockchain	Smart Contract
S3	2015	*Decentralized Reputation System for Transaction Networks*	Trust and Reputation Systems
S4	2014	A next-generation smart contract and decentralized application platform	Smart Contract
S5	2018	How to build a reputation system on blockchain	Blockchain based reputation systems
S6	2016	Fraud detections for online businesses: a perspective from blockchain technology	Blockchain-based Reputation Systems
S7	2015	Feedback-based reputation on top of the bitcoin blockchain	Blockchain-based Reputation Systems
S8	2017	Under-optimized smart contracts devour your money	Smart Contract
S9	2016	Blockchains and smart contracts for the Internet of Things	Smart Contract
S10	2018	Blockchain disruption and smart contracts	Blockchain-based Reputation Systems
S11	2013	Information propagation in the bitcoin network	Blockchain-based reputation Systems
S12	2016	Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab	Smart Contract
S13	2016	Replacing paper contracts with Ethereum smart contracts	Smart Contract
S14	2016	From institutions to code: towards automated generation of smart contracts	Smart Contract
S15	2018	Blockchain and smart contracts for insurance: Is the technology mature enough?	Smart Contract
S16	2016	Evaluation of logic-based smart contracts for blockchain systems	Smart Contract
S18	2016	The ring of gyges: investigating the future of criminal smart contracts	Smart Contract
S19	2018	Incorporating seller/buyer reputation-based system in blockchain-enabled emission trading application	Blockchain-based Reputation Systems
S20	2016	Hawk: The blockchain model of cryptography and privacy-preserving smart contracts	Smart Contract
S21	2017	Smart contracts–How will blockchain technology affect contractual practices?	Smart Contract
S22	2017	Validation and verification of smart contracts: A research agenda	Smart Contract
S23	2016	Setting standards for altering and undoing smart contracts	Smart Contract
S24	2016	A trustless privacy-preserving reputation system	Blockchain-based Reputation Systems
S25	2016	Reputation and feedback systems in online platform markets	Trust and Reputation Systems
S26	2014	Challenges and opportunities associated with a bitcoin-based transaction rating system	Trust and Reputation Systems
S27	2016	Blockchain contract: securing a blockchain applied to smart contracts	Blockchain-based Reputation Systems
S28	2018	Smart contracts: security patterns in the Ethereum ecosystem and solidity	Smart Contract
S29	2014	Ethereum: A secure decentralized generalized transaction ledger	Blockchain-based Reputation Systems
S30	2015	Decentralizing privacy: using blockchain to protect personal data	Trust and Reputation Systems

Table 3
Descriptions, issues and limitations of existing studies on trust and reputation systems.

Study	Description of the Study	Issues/Limitations	Requirements of a Smart Contract				
			Req 1	Req 2	Req 3	Req 4	Req 5
S3	Developed a reputation algorithm called net flow convergence and a decentralized system that calculates reputation based on underlying network structure and allows users to look up and record the histories of transaction outcomes. The network inflow or outflow is the sum of complete set of edges, along with edge weight.	The system can only be used by researchers and programmers. For the theoretical utility of the system to be seen, it needs to reach widespread use. Not accurate enough to verify real-world reputation; a future system could use web crawlers to link nodes in the transactional network	✓	✓	X	X	✓
S25	Describes how reputation helps facilitate trust and trade and explores some of the problems of bias in feedback and reputation systems.	Various solutions provided were not implemented in real-world scalability	X	X	✓	✓	X
S26	Considers three different models by which a reputation/ rating system could be implemented in conjunction with Bitcoin transactions and considered the pros and cons of each. The paper found that each model faces challenges on both technological and social fronts. The rating system models examined includex site-based systems, coin-based systems and wallet-based systems.	Some questions were not answered in the study. For example, can a site-based rating system interact with external wallets?	✓	✓	X	X	X
S30	Describes a decentralized personal data management system that allows users to take charge and control their own data.	The analysis only paid attention to storing pointers to encrypted data. Even though the approach is appropriate for random and storage, it is not effective or efficient for processing data.	X	X	X	X	X

The records are excluded if:

1. They are duplicate reports of a similar study.
2. Informal literature reviews that have no defined research questions, no defined data extraction process, or no defined search process.
3. They are not written in the English language

The stages of evaluating and selecting the relevant papers for SLR are summarized in Table 1.

From the 109 papers remaining from the previous step, the titles of the studies were evaluated to find only those that included the search terms; this further reduced the number to 88. Finally, the abstracts of the papers were read and evaluated to eliminate irrelevant papers. After this evaluation, the number of papers reduced to 38.

3.3. Step 3: quality evaluation

The 38 selected papers from the knowledge record were retrieved and critically evaluated based on the three quality evaluation questions, as follows:

QE1: Does the paper cover relevant work and explore the research topics comprehensively?
QE2: Does the paper provide clear findings with justifiable results and conclusions?
QE3: Does the paper provide future directions?

Any paper which has at least two 'yes' answers to the three evaluation criteria questions is included in this SLR. Of the 38 papers, 30 of them satisfied the criteria as shown in Table 2.

3.4. Step 4: shortlisted papers for SLR and categorizing them into broad areas

Each of the shortlisted papers was analyzed according to its scope, topic area, author's information, country and the summary of its research questions and answers. Based on the analysis, the selected papers were categorized into one of the broad areas of *trust and reputation systems*, *blockchain-based reputation systems* or *smart contracts,* as shown in Table 2. These areas were chosen as they are broadly related to the areas from where the requirements (Req 1 to Req 5) to facilitate a smart contract arise. The papers in each area are summarized in the next section and their issues and limitations with respect to the key requirements (Req 1 to Req 5) needed from a smart contract, as defined in Section 2, are discussed.

4. Analysis of shortlisted papers against the requirements to facilitate a smart contract

4.1. Trust and reputation systems

Online reputation systems represent an important kind of mechanism for establishing trust between interacting parties. According to Hendrikx et al. (2015), reputation systems facilitate trust between entities by increasing the effectiveness and efficiency of online services and communities. Such systems are increasingly gaining acceptance by players in different sectors such as health, transportation, finance etc. and are thus becoming an essential fabric of different websites and online services. A great potential exists for online trust and reputation systems and they can be implemented across different sectors. Reputation systems represent a trend when it comes to decision support systems for services offered through the Internet (Dennis and Owenson, 2016). The basic idea of reputation systems is that they allow various users to rate each other after a transaction is completed and show an aggregate rating of a user to provide a reputation score (for the service provider and the service requestor). This reputation score is used by other users to make decisions about whether they should engage with the user providing the service in the future. Dennis and Owenson (2016) argue that such systems provide an incentive for good behavior within a market, thus ensuring that there is good market quality. For service providers to build their reputation value, they must first build trust. Guy et al. (2015) used two definitions of trust: *'decision trust'* and *'reliability trust'*. Reliability trust can be defined as the infallibility of an individual or something (Guy et al., 2015). Trust is, therefore, the relative probability that a *User A* expects another *User B* to perform a given action on which the welfare of User A depends. However, due to the complex nature of trust, it becomes difficult to make a decision on whether to enter into a situation of dependence with another individual or not. On the other hand, decision trust is defined as the extent to which a user is willing to depend on an individual or something at a given time with a feeling of subjective security, even in the case that negative consequences may occur. The abstract nature of decision trust is what provides a foundation of the broader notion of trust which includes dependence on the trusted party.

Table 4
Descriptions and limitations of studies on blockchain-based reputation systems.

Study	Description	Issues/Limitations	Requirements of a Smart Contract				
			Req 1	Req 2	Req 3	Req 4	Req 5
S5	Developed Bitconch chain, a new distributed web protocol using an innovative proof of reputation consensus algorithm. To build reputation on blockchain, the Bitconch chain mathematically models time, contribution activities and social network. Technologies used in achieving decentralization and scalability include Zero Knowledge-Proof, post-quantum encryption algorithm, directed acyclic graph etc.	Inability to bootstrap new users. The proposed model does not solve the problem faced by service providers who want to transfer reputation.	✓	✓	X	X	✓
S6	This study explores rating fraud by differentiating subjective fraud from objective fraud. Then, it discusses the effectiveness of blockchain technology in objective fraud and its limitations in subjective fraud, especially rating fraud. The paper also carried out a systematic analysis of a blockchain-based reputation system in both objective fraud and subjective fraud.	Ballot stuffing, whitewashing attacks, and camouflage attacks, inability to bootstrap new users, cannot carry out context-based trust assessment and no predictive analytical approach to predict future trust value.	X	X	✓	✓	X
S7	This paper shows how a decentralized and distributed feedback management system can be built on top of the bitcoin blockchain. The primary objective of the paper is to avoid giving the control (centralization) of the feedback management system to internet firms alone.	Fake identities, not collusion resistant, Sybil attacks, inability to bootstrap new users, cannot carry out context-based trust assessment and no predictive analytical approach to predict future trust value.	✓	X	X	X	X
S10	Analyzes how decentralization improves consensus effectiveness, and how the quintessential features of blockchain reshape industrial organizations and the landscape of competition.	The paper did not design a robust consensus protocol nor did it provide the right incentives for maintaining consensus on specific blockchains.	X	✓	✓	X	X
S19	Incorporates blockchain technology to address the management of the emission trading scheme (ETS) and fraud issues and utilizes a reputation system in a new approach to improve ETS efficacy. A multi-criteria analysis was carried out to evaluate the proposed scheme in comparison to conventional ETS model. The result of the analysis showed that the proposed model is more efficient.	Attacks against reputation systems, like bad-mouthing, ballot stuffing etc.	✓	X	✓	X	✓
S24	This paper presents a blockchain-based trustless reputation system and analyzes its correctness and the security guarantees it promises; and eliminates the need for users to trust fellow users or any third party. The paper used a blinded token exchange algorithm to verify that a customer was involved in a transaction before allowing such customer to rate the service provider.	Attacks against reputation systems, like bad-mouthing, ballot stuffing, Sybil attacks, and whitewashing. Others are inability to bootstrap new users, and no predictive analytical approach to predict future trust value.	✓	✓	X	X	✓
S27	This paper proposes a new mechanism for securing a blockchain applied to contract management such as digital rights management. The study designed a new protocol that can be used to record a trail of consensus on the blockchain. A transaction is used as evidence of contractor consent in this protocol.	The mechanism was not implemented on actual cryptocurrency.	X	✓	X	✓	X
S29	The paper discusses the design of Ethereum, its implementation issues, the opportunities it provides and future problems.	Scalability remains an ongoing concern. With a generalized state transition function, it becomes difficult to partition and parallelize transactions to apply the divide-and-conquer strategy.	X	✓	X	X	X

Trust and reputation systems on the Internet are motivated by several things. One of these motivations is to find useable substitutes for traditional signs of trust and reputation. Another motivation is to leverage the Internet infrastructure to develop efficient platforms or systems to collect ratings for service providers and derive reputation values to provide fundamental decision support systems to improve the quality of online platforms (Monir et al., 2013). There are several situations where some users are known for giving poor feedback to service providers. This is inimical to the reputation scores of service providers. Reputation systems should have an algorithm that can be used to model the trust values of a service provider. To achieve this, Resnick and Zeckhauser (2015) considered the following three properties that should be included in all reputation systems.

a) All entities in such reputation systems must be long-lived ensuring that in each transaction, there is an expected transaction by those entities in the future
b) All ratings for the present interactions should be distributed, and
c) The ratings for past interactions must be used as the decision-making basis for present-day transactions.

Table 3 presents a summary of the approaches that fall under the trust and reputation category and their commitment to the requirements of a smart contract.

4.2. Blockchain-based reputation systems

Blockchain, a technology on which Bitcoin has been implemented (Xu et al., 2017), can be used to address the issues surrounding reputation or review fraud. According to English et al. (2016), blockchain is a database that is transactional and globally shared, which is like the BitTorrent. The blockchain database can be accessed by all participants in the network. For those functions that need auditability, provenance and trusted computing, blockchain technology can be efficiently used (Zyskind and Nathan, 2015). The blockchain system can be applied to various domains. This technology utilizes a decentralized ledger (Khaqqi et al., 2018). As all transactions must be publicly broadcasted and be permanent, it can provide various types of services, such as product or service delivery verification in the supply chain industry, educational qualification verification in the education industry, money transfer security in the financial industry, and payment chargeback risk mitigation in e-commerce (Khan, 2015). Another important application area for

blockchain systems is financial fraud detection.

To facilitate business decision making, a variety of decision support systems (DSS) have been built in several domains or sectors. Given the information provided by users, a decision is made based on the decision-making model which may have built-in rules. Such systems significantly improve the effectiveness and efficiency of decision making, although they are vulnerable to manipulated (or fraudulent) input information, such as loan fraud (Zyskind and Nathan, 2015). For example, a decision on a loan application can be generated based on inputs of customers' personal information. When a user intends to apply for a loan through an online application system, he/she may falsify some of their personal financial information, such as a fake repayment history, thus increasing the possibility of acceptance. Consequently, financial institutions may suffer tremendous losses due to loan fraud. Blockchain systems can keep historical transactions records that form input to DSS. The applicants cannot falsify information to obtain a favorable decision. Of all the application areas, we focus on the applications on rating fraud detection in the subsequent section.

In addition to the issues discussed above, reputation systems can also be treated as digital currency using blockchain. Through this, the reputation value of an entity will not be glued to a platform, instead, it will be platform agnostic. That is, a service provider has the opportunity to transfer reputation from one platform to another thereby ensuring that the reputation they have earned is not lost. Also, there will be an opportunity for reputation exchange and the bootstrapping of new users.

According to Coleman (2016), the seller is likely to promote his/her own product by encouraging people who provide fraudulent ratings to complete real transactions. These people may be offered free or significantly discounted products to solicit a positive review. This phenomenon has already been noted by Amazon.com. Amazon has removed the "verified purchase" badges from reviews associated with discounted transactions (Coleman, 2016). Furthermore, sellers can allow customers to first pay the full amount, submit ratings, and pay them back in other ways. Although transaction records are incorruptible in the blockchain-based reputation systems, fraudulent raters in such false "real transactions" are not detected. Cai and Zhu (2016) noted that although reputation systems are designed to serve as a mechanism that will reduce the risks related to online shopping, it is vulnerable to rating fraud. This fraud includes a situation where some raters will input unfairly low or high ratings into the system just to demote their competitors or promote their own products. They then explored the limitations of blockchain technology in subjective fraud and its effectiveness in objective fraud and concluded that blockchain-based reputation systems are efficient when they are deployed to prevent objective fraud, such as a loan application where the fraudulent information is fact-based. However, they noted that the effectiveness of blockchain-based reputation systems is limited in subjective information fraud where any ground-truth cannot be strongly confirmed.

Schaub et al. (2016) proposed how to utilize digital signatures to design reputation systems that can protect users' privacy. In a similar manner, Soska et al. (2016) proposed a system "Beaver", which protects users' privacy, while being resistant against Sybil attacks by charging fees. Dennis et al. (2016) designed reputation systems with underlying blockchain technology. These systems generate and broadcast a binary P2P rating on receiving the correct file. Table 4 presents a summary of the approaches that come under the blockchain category and their commitment to the requirements of a smart contract.

4.3. Smart contracts for reputation systems

According to Lauslahti et al. (2017), smart contracts are algorithmic, self-enforcing, and self-executing computer programs. These smart contracts eliminate the necessity of a trusted third party in transactions by allowing untrusted parties to manifest contract terms (Wohrer and Zdun, 2018).

Cong and He (2018) explained how decentralized ledger technologies such as blockchains can simplify the creation of smart contracts. Furthermore, using smart contracts, the users are able to codify precisely their trust relations and agreements. These will be automatically executed by platforms like Ethereum after deployment. In fact, these smart contracts can facilitate economic activities by effectively providing services that are offered traditionally by intermediaries (e.g., notaries, bank, and courts) and trusted third parties. In order to secure blockchains, Watanabe et al. (2016) proposed a new mechanism based on smart contracts that can be implemented in contract management. A new consensus method was used in this mechanism that used credibility scores to create a hybrid blockchain. In this way, it is possible to thwart attackers from monopolizing resources and thereby ensure the security of the blockchains (Everts and Muller, 2018). Cong and He (2018) also opined that with a large range of economic outcomes, smart contracts and blockchain can sustain market equilibria. Bigi et al. (2015) noted that protocols based on decentralized smart contracts can facilitate interaction among independent players without the interference of any coercing authority. The authors believed that these smart contracts could even be used in various applications in the future as a potentially enabling technology. This makes it essential to validate this technology. Hence, the authors combined formal models and game theory for validating such bitcoin-based systems based on smart contracts. Christidis and Devetsikiotis (2016) examined the usefulness of using smart contracts and blockchains in Internet-of-Things (IoT) domain. The authors found that the powerful blockchain-IoT combination can cause substantial transformations across multiple industries. This can result in the creation of new distributed applications and business models. Kosba et al. (2016) presented a decentralized smart contract system called 'Hawk'. This new system can guarantee transactional privacy by ensuring that the system does not store information about financial transactions on the blockchain. In this way, it can help different parties to transact safely as the transactions are not exposed.

In order to coordinate interactions between independent entities, like humans, agents, etc., Frantz and Nowostawski (2016) discussed the potential of blockchain technology. Blockchain technology often faces the challenge of ensuring the broader use of the correct and unambiguous specification of smart contracts (Toneli et al., 2018). The authors introduced a process to automate institutional constructs into rules that are contractual and machine-readable. Using this process, people with different levels of technical background will be able to easily generate smart contracts and use blockchain technology as an efficient coordination tool. Buterin (2014) and Wood (2014) discussed a smart contract platform called Ethereum. The authors highlighted the issues regarding its design, implementation, and also the opportunities it provides. Some of the common security patterns on Ethereum were discussed by Wohrer and Zdun (2018). These included Checks-Effects-Interaction, Emergency Stop (Circuit Breaker), Speed Bump, Rate Limit, Mutex, and Balance Limit. Developers can address security problems like harmful call-backs and uncontrollably high financial risks by applying these patterns. A Smart Contract-based Public Key Infrastructure (SCPKI) was proposed by Al-Bassam (2017). The SCPKI uses a transparent and decentralized design using a smart contract and a web-of-trust model on the Ethereum blockchain. The author argued that this PKI system is capable of detecting rogue certificates when they are published. In this way, it would be possible to ensure secure communication on the Internet.

Marino and Juels (2016) defined a new set of standards for undoing and altering smart contracts as traditional tools often fail in this regard. The authors developed a new set of standards and tried to prove their worth after applying to Ethereum, a popular smart contract platform. In the end, they succeeded in their approach and proved the value of such a framework. Idelberger et al. (2016) found the technical and legal advantages of using logic-based languages instead of procedural languages for programming smart contracts in the blockchain system. The authors concluded that smart contracts based on logic-based languages are easier for developers to work with. Furthermore, logic-based smart

Table 5
Descriptions, issues and limitations of existing studies on smart contracts.

Study	Description	Issues/Limitations	Requirements of a Smart Contract				
			Req 1	Req 2	Req 3	Req 4	Req 5
S1	Smart contract-based public key infrastructure (SCPKI) is a substitute PKI system built on a transparent and decentralized design using a smart contract on the Ethereum blockchain and a web-of-trust model, to make it easily possible for rogue or fake certificates to be detected when they are published. The developed web of trust/confidence model is decentralized and highly fault-tolerant.	Issues related to privacy. The system is only appropriate for publishing attributes that the user wishes to make public. It is not suitable for publishing more private identity attributes such as a personal address. Issues related to adaptability. The design of the system is such that all parties referenced by the system must already use the system.	X	X	✓	✓	X
S2	Demonstrated a decentralized app (DAPP) for the distribution of everyday objects based on a smart contract on the Ethereum blockchain. This contract allows users to register and rent devices without involving any trusted third party (TTP), the revelation of any personal information or prior signup to the service.	The paper identified significant fees for users and overbearing terms and conditions as part of the problems of the sharing economy but did not provide any solution for them.	X	X	X	X	X
S4	Created Ethereum, an alternative protocol for building decentralized applications. It is a blockchain with an in-built language that allows users to write smart contracts and create their own transaction formats.	Rudimentary Ethereum virtual machine implementation, primitive architecture and underdeveloped language. Ethereum is less-optimized for one specific use case.	X	X	✓	✓	X
S8	The paper found out that smart contracts that are under-optimized cost more gas than normal thereby overcharging users. To address this, the study developed GASPER, a new tool to automatically locate costly gas patterns by analyzing the bytecodes of smart contracts.	The compilers need to be improved to produce gas-efficient bytecode.	X	✓	X	X	X
S9	Reviewed how a blockchain-IoT combination can facilitate the sharing of resources and services thereby leading to the creation of a marketplace for devices and users. It also discussed how the combination allows automation of many time-consuming workflows in a cryptographically verifiable manner. The issues and challenges that need to be addressed before the deployment a blockchain-IoT system were also identified.	The paper did not provide specific solutions to most of the challenges identified.	X	X	X	✓	X
S12	Discussed the common pitfalls in designing safe and secure smart contracts and how to fix them. This was based on insights gathered through years of pedagogical efforts on smart contracts.	Did not include programmers' learning adversarial thinking through attacking and amending their own code	X	X	✓	✓	X
S13	Identified what criteria Ethereum needs to fulfill to replace paper contracts. It discussed the privacy and security of the blockchain. The paper noted that it is not recommended to place paper contracts on Ethereum blockchain because of the huge privacy lapses and the variety of contract clauses.	The study did not provide any solution to privacy setbacks and the security issues identified.	X	X	✓	X	X
S14	Proposed a modelling approach that supports the semi-automated translation of human-readable contract representations into computational equivalents in order to enable the codification of laws into verifiable and enforceable computational structures that reside within a public blockchain. The paper identified smart contract components that are obtainable in real-life institutions and proposed a mapping which was executed using a domain specific language.	Failed to explore the possibility of reversal, that is, given a blockchain contract, is it possible for humans or autonomous entities to verify the actual contractual semantics and obligations?	X	✓	X	X	✓
S15	Presented an overview of potential applications and use cases of blockchain and smart contracts in the insurance sector. Also, the paper provided a more general SWOT analysis of blockchain.	Study is restricted to the insurance sector alone.	X	✓	✓	X	X
S16	Provided insights on how to use logic-based smart contracts in combination with the blockchain. network. The paper noted that algorithms for logic approaches need to be efficient in the specific environment they are deployed. This was illustrated using various algorithms from defeasible logic-based frameworks.	While the paper identified procedural language as the most commonly used language to program smart contract, it does not justify why using logic-based languages will be a better alternative.	X	X	X	✓	✓
S17	Decentralized smart contracts represent the next step in the development of protocols that support the interaction of independent players without the presence of a coercing authority. The paper combined game theory and formal models to tackle the new challenges posed by the validation of decentralized smart contracts. The probabilistic framework adopted allowed to properly model of uncertainty and non-determinism in players' behavior. It also helped in exploiting statistical model checking to validate the smart contract.	The paper did not solve the problem of more complex and repeated games which require smart contracts exhibiting more sophisticated behavior.	X	X	✓	✓	✓
S18	Explored the risk of smart contracts that can cause new criminal issues and demonstrated significantly that Criminal Smart Contracts (CSCs) for the leakage of secrets are	Discussed only few Criminal Smart Contracts and did not point out potential countermeasures.	X	X	✓	X	X

(*continued on next page*)

Table 5 (*continued*)

Study	Description	Issues/Limitations	Requirements of a Smart Contract				
			Req 1	Req 2	Req 3	Req 4	Req 5
	efficiently realizable in existing scripting languages such as that in Ethereum.						
S20	Presented Hawk, a decentralized smart contract system that does not store financial transactions on the blockchain, thus retaining transactional privacy from the public's view.	Not integrated with any reputation system.	X	X	✓	X	X
S21	The paper examined how the formation mechanisms of the general principles of contract law can be applied to the new technological framework of smart contracts.	Although this paper has described three examples of smart contracts, in reality, the number of possible applications may be practically infinite.	X	X	X	X	X
S22	This paper explored the issues and research challenges faced in the authentication and confirmation of smart contracts, especially the ones that run over blockchain.	Not integrated with any reputation system.	X	X	✓	X	X
S23	This paper developed a new set of principles for changing and undoing smart contracts and thereafter applied these principles to a smart contract in existence.	No predictive analytical approach to predict future trust value.	X	X	X	X	X

contracts can also reduce the risk of errors in the implementation. In addition, it is possible to ease the validation process by using this particular type of smart contract. Lauslahti et al. (2017) analyzed smart contracts from the context of Finnish contract law and digital platforms. The authors found that smart contracts can be applied in a variety of ways, with different circumstances and goals. They concluded that smart contracts could generate legally binding obligations and rights to their parties, at least in some cases. Gatteschi et al. (2018) tried to help insurers decide whether to adopt blockchain technology or not by clarifying the concepts of blockchain and its advantages and disadvantages. The authors argued that blockchains and smart contracts can improve customer experience and reduce operating costs, minimize the overhead related to the verification of new customers and manual data entry, compute risk assessments and prevent frauds. Table 5 presents a summary of the approaches that come in the smart contract category and their commitment to the requirements needed for the facilitation of a smart contract.

4.4. Research gaps in the existing studies from the requirement perspective of a smart contract

As presented in Tables 3–5, researchers have focused on forming and facilitating smart contracts. However, from the perspective of *before* and *after* phases of a smart contract, the existing work has the following drawbacks:

- *Inability to derive the reputation value of service providers based on their performance in earlier smart contracts:* While existing work has focused on integrating reputation values with Bitcoin transactions (S26), they do not focus on using these values for other transactions. This is required in the *before* phase of a smart contract, where a user's need may be in different requirements from what the provider's value is in. To this end, (S3) focused on using the underlying network structure to calculate the reputation value, but not on how it can be interpreted in other contexts. (S30) proposed an approach for using decentralized data but that is for a user's own value and not for service providers. Without such an approach, the existing literature does not allow the service user to determine the reputation value of a provider in the context of forming a smart contract.
- *Inability to deduce the trust value of service provider in a specific context:* Another aspect which is required by a service user in the *before* phase of a smart contract is the ability to deduce the performance of a service provider in a specific context. While (S10) does initial work on investigating the use of decentralization, it does not represent how to use these values to transform it into context-specific requirements. Other researchers such as (S29, S27) proposed technologies for forming smart contracts, while others such as (S14, S8) focus on the technical aspects of forming one, but they focus on the *during* stage and not on the *before* aspects required for forming a smart contract.
- *Reputation system as a digital asset and moving across platforms:* The third requirement to facilitate smart contracts across different platforms is to enable service providers to move their reputation values across different platforms. This can be done when the reputation value is regarded as a digital asset and can be moved across platforms. While (S25) mention how reputation value helps to facilitate trade, it discussed how it can be transferred or moved. Other studies such as (S19, S24, S1, S4, S15) utilize blockchain in a specific domain but do not mention how it can be transferred across others. (S13) mentions privacy and security aspects as the key requirements to be addressed in a smart contract. These are more focused in the *during* stage of the smart contract but fail to mention how these can be achieved in the *before* stage, if such values are unable to be transferred across platforms.
- *Detection of non-compliant behavior:* The monitoring of non-complaint behavior has been studied widely in the literature. Studies such as (S6) investigated rating fraud by differentiating it with subjective fraud and objective fraud. Other approaches such as (S1) used the PKI system to detect fake certificates. (S17, S20) used a game theory-based approach to detect uncompliant behavior and a privacy-based approach respectively in a decentralized environment while (S18) used a secure environment to prevent leakage. However, the existing approaches focus on the *during* part of the smart contract and do not mention how to prevent inflating the existing reputation values on which the analysis in the *before* and *after* phases of the smart contract are built. Without these, the existing approaches cannot ensure that the shown values are indeed correct and free from bias.
- *Mathematical models and algorithms:* Some of the papers examined, like S3, S5, S17, S19 and S24, utilized mathematical models and algorithms to compute reputation values. (S3) developed a reputation algorithm called net flow convergence and a decentralized system that calculates reputation based on underlying network structure. (S5) mathematically modeled contribution activities, time and social network to build a decentralized reputation system. The model was established using a proof of reputation consensus algorithm. (S19) uses an algorithm called priority value (PV) to help buyers sort bids from sellers. (S24) made use of a blinded token exchange algorithm to verify that a customer was involved in a transaction before allowing such customer to rate the service provider. Finally (S17) adopted a probabilistic framework which allowed a proper modelling of uncertainty and non-determinism in players' behavior and it also helped in exploiting statistical model checking to validate the smart contract. However, the existing work only focused on the *before* and *during* phases of smart contracts. None of the papers in the examined or provided a reputation algorithm that can be

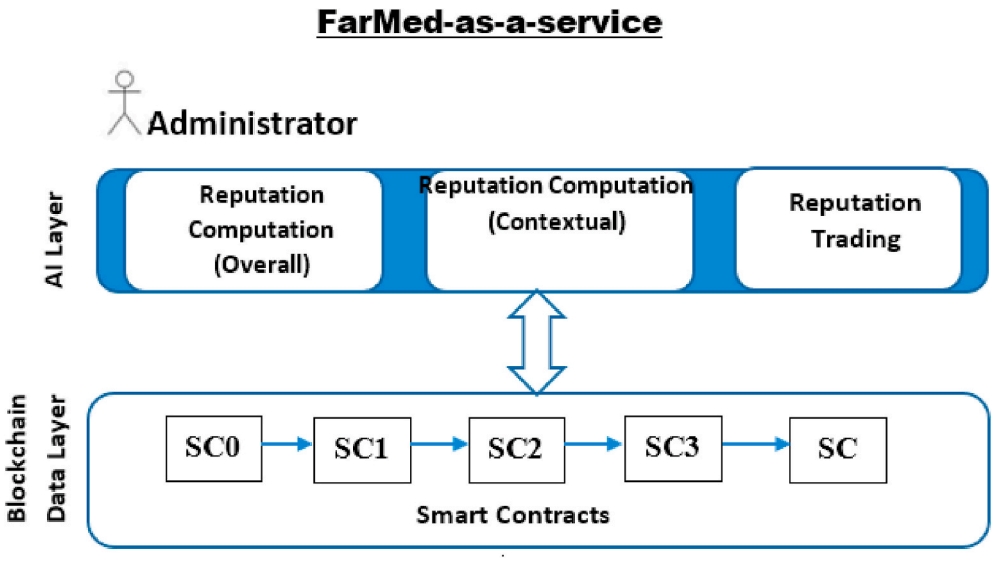

Fig. 3. Details of the FarMed service.

utilized to compute the remaining reputation values of service providers *after* reputation trading or auctioning.

In the next section, we present our proposed framework to address the gaps.

5. Smart contracts-based reputation system service framework

This section discusses the methodological approach that is used to address the gaps identified in the literature. The proposed framework is termed *FarMed Service*, which is a smart contracts-based reputation system service framework that is driven by service-oriented computing (SOA). The framework is divided into two layers as shown in Fig. 3.

Layer 1 – Blockchain data layer: In this layer, Ethereum-smart contracts verify that the reputation values of service provider/s and buyer/s have not been manipulated. Smart contracts in this layer store all the reputation values of all service provider/s and buyer/s.

Layer 2 – AI layer: This layer computes the analysis from information embedded in the smart contracts. In this layer, once data is acquired, it is passed to different intelligent modules to update the rating value of the service provider or buyer. The different modules that are in this layer are reputation computation, reputation predictive analytic, reputation trading and reputation auction service.

Fig. 4 shows the working of the FarMed framework from the stage of the user visiting the e-market to select an item to purchasing or canceling the purchase intent. There are three phases namely the *marketplace phase*, *smart contract execution phase* and *trust value computation phase* in the FarMed framework. The *marketplace phase* represents the series of steps needed by the client to form a contract. Once a contract is formed, the workflow for the *smart contract execution phase* of the framework as shown in Fig. 5 is executed. Taking the example of contract *C*, Fig. 5 shows its initialization and the execution of its logic. X is the condition that a purchase which has not been rated exists. Z is the condition that a rating value has been provided by the service consumer. If any of conditions X and Z are not met, the smart contract execution will automatically fail. For the execution of the contract to be completed, both conditions X and Z must be met. When both these conditions have been met, the operation address Q is executed. This phase fulfills requirement 4 stated in section 2.4. This leads to phase 3, which is the *trust value computation phase*. As shown in Fig. 4, this phase addresses requirements 1, 2, and 3 mentioned in sections 2.1, 2.2 and 2.3 respectively and includes the development of intelligent methods to compute overall reputation of service providers, compute reputation of a service provider in a context and allow service-provider reputation transfer. To achieve requirement 1, a five-star algorithm to compute and represent the service provider's reputation will be used in FarMed. For requirement 2, service ontology and AKTiveRank algorithm (proposed by Alani and Brewster, 2006) are used for context-based trust inferencing.

The AKTiveRank uses four types of measures or assessments for each ontology to measure/assess the similarity distance. These include the Class Match Measure (CMM), Semantic Similarity Measures (SSM), Betweenness Measure, and Density Measure (Alani and Brewster, 2006). Finally, the EigenTrust algorithm will be used to address requirement 3. A brief description of how the FarMed framework aims to address the key requirements defined in Section 2 for the Smart Contract to address is explained in the next sub-sections.

5.1. Modelling and deducing the overall reputation value of service providers (Req: 1)

There is a need to model the overall reputation value of service providers based on the trust values stored in the smart contracts. To do this, a reputation algorithm will be used. The procedure involved in satisfying this requirement is shown in phase 3 in Fig. 5 above. It involves getting the prior ratings of the service provider from FarMed and computing an updated reputation value which is then stored in FarMed.

5.2. Modelling and deducing the trust value of service providers within a context (Req: 2)

To model the reputation value of a service provider in a context, FarMed in the trust value computation phase develops a service ontology coupled with AKTiveRank (a semantic distance-based algorithm proposed by Alani and Brewster, 2006). The current architecture of the AKTiveRank is shown in Fig. 6. The main component of the architecture is a Java Servlet (No. 2 in the figure) which gets a text query from marketplace (No. 1). The text, which is product name, to be searched for is in the query. Meanwhile, it is important to note that the product name will only be matched with ontology classes rather than with comments or properties. When AKTiveRank (No. 2) receives a query, it will query Swoogle (No. 3) for all the product names provided and retrieve the Ontology Uniform Resource Identifiers (URIs) from the returned results (Fensel et al., 2000). Swoogle is an ontology search engine that adopts a PageRank-like method to rank ontologies by analysis links and referrals between the ontologies to identify the most

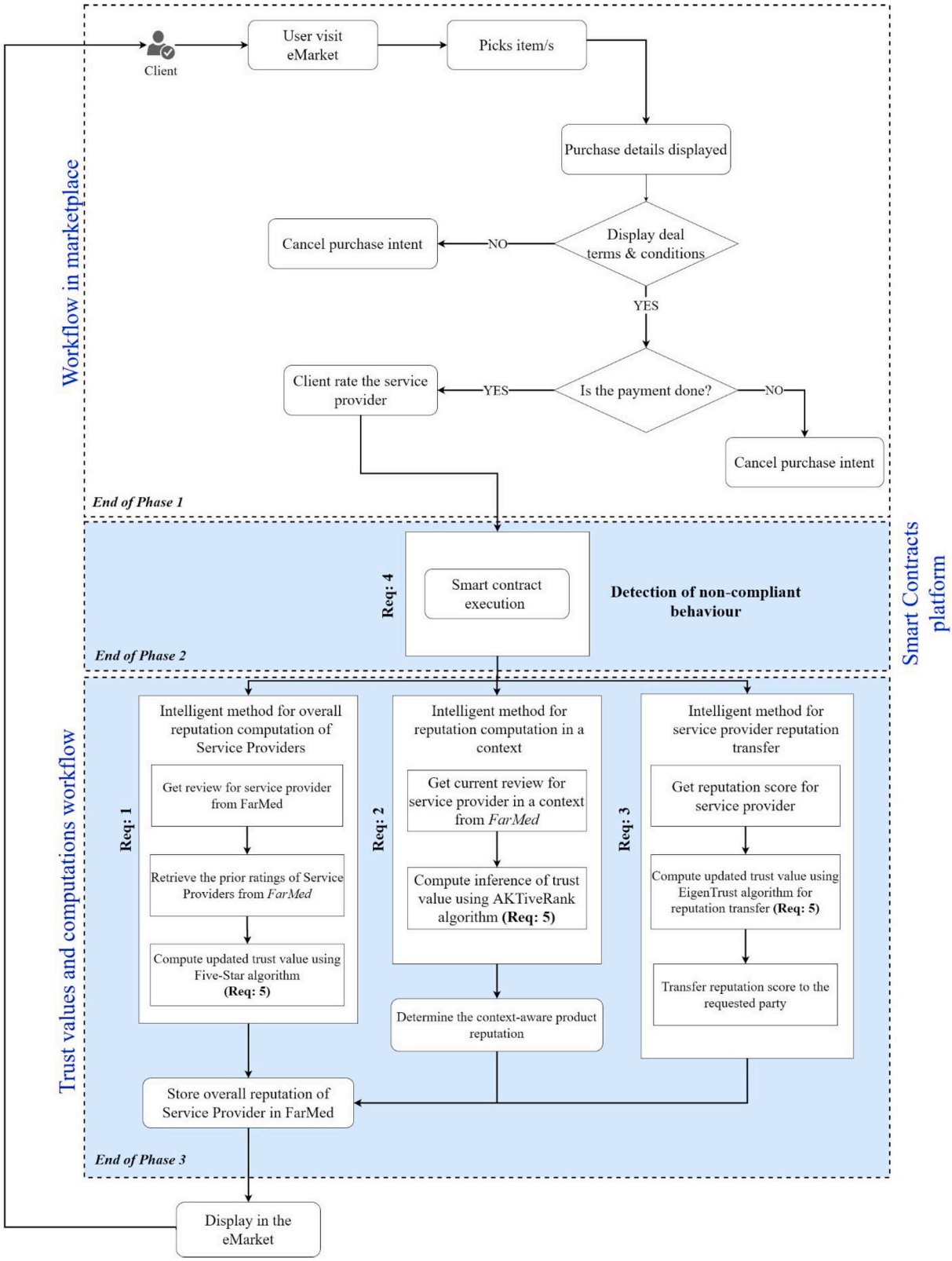

Fig. 4. Flow of control in the phases of (a) marketplace (b) smart contract execution and (c) trust value computation of the FarMed framework.

relevant ones (Gomez-Perez and Corcho, 2002).

After gathering a list of ontology candidates from Swoogle, AKTiveRank will check whether the ontologies are stored in a Jena MySQL database back-end (No. 4). For any ontology that is not in the database, AKTiveRank will download them from the web (No. 5) and add to the database (Alani and Brewster, 2006). The Jena API is used to read the ontologies as well as handle the database. According to Angles and Gutierrez (2005), the existing Resource Description Framework (RDF) queries languages are not suitable for graph queries. Therefore, the AKTiveRank is connected to a purpose-built JUNG servlet (No. 6). This

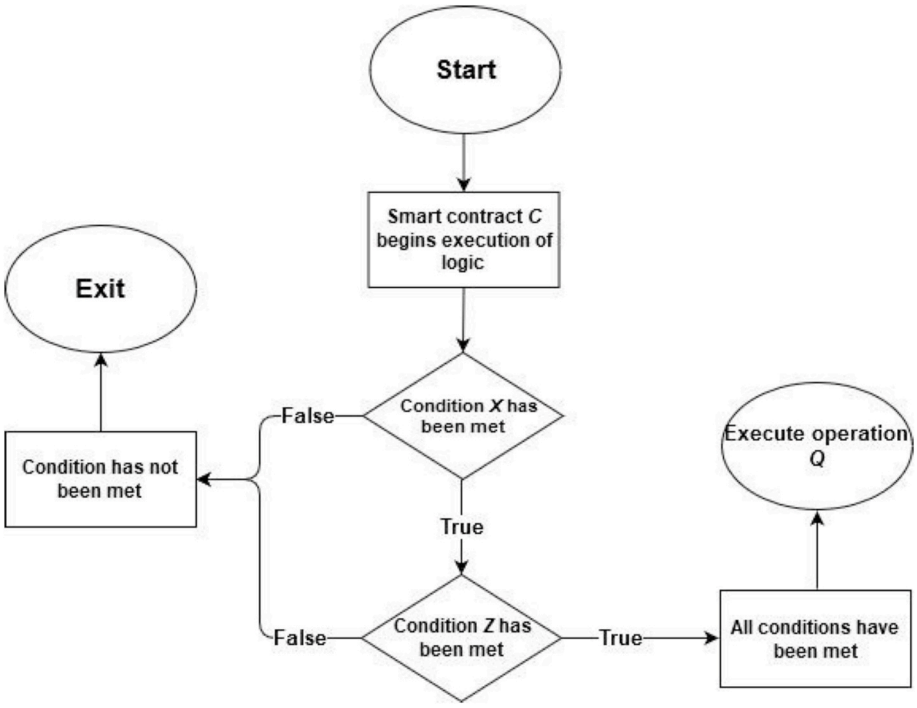

Fig. 5. Sequence of working of the Smart contract execution phase of FarMed framework.

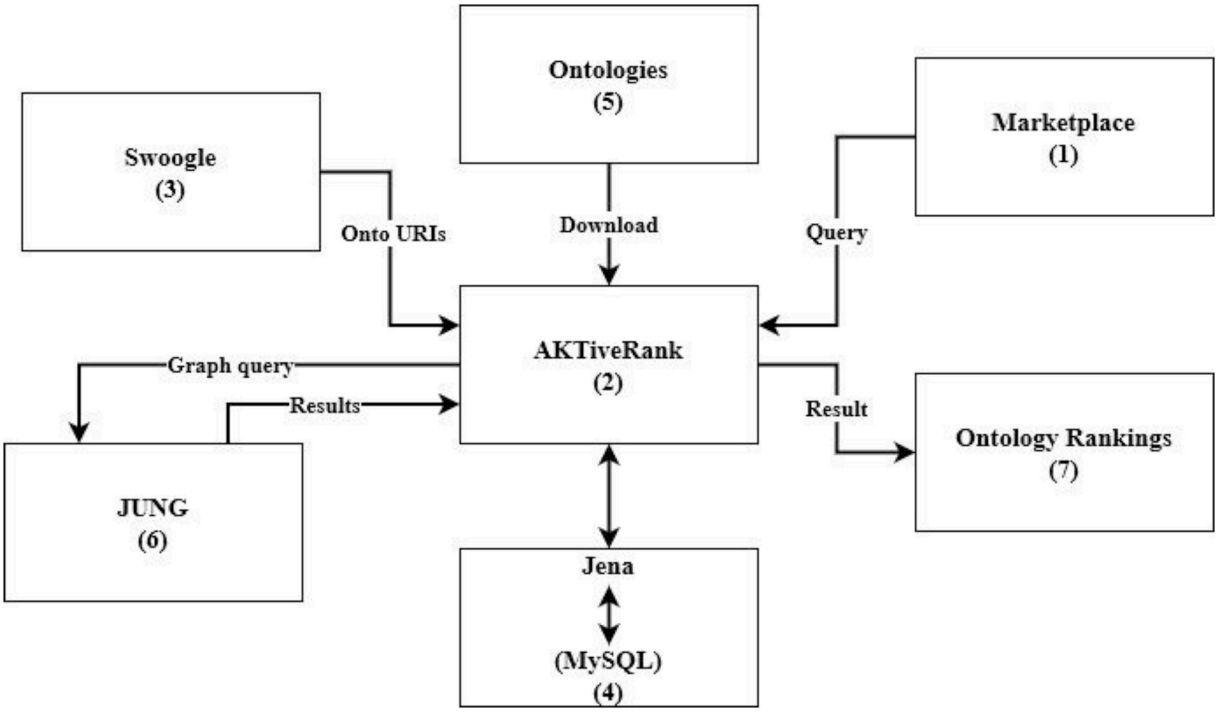

Fig. 6. AKTiveRank architecture (Alani and Brewster, 2006).

servlet gets an ontology URI and returns the results of JUNG queries in RDF. JUNG, which stands for Java Universal Network/Graph framework, is a software library that is used for visualizing and analyzing network graphs (Alani and Brewster, 2006).

5.3. *Transferring reputation among service providers and across platforms (Req: 3)*

In order to bootstrap new service providers in the reputation-based economy, FarMed in the trust value computation phase will introduce the concept of *Reputation Auction*. The intention of this proposed method is that service providers with high or excess reputation values will auction part of their reputation ratings to other service providers and will receive payment for doing so. This is clearly demonstrated by Req: 3 in the phase 3 of Fig. 4. The new sellers who have a zero-reputation score can buy from this auction to build their reputation in the market quickly while the offers in the auction will be made by sellers who usually have a high reputation score. The benefit for those who sell full or part of their

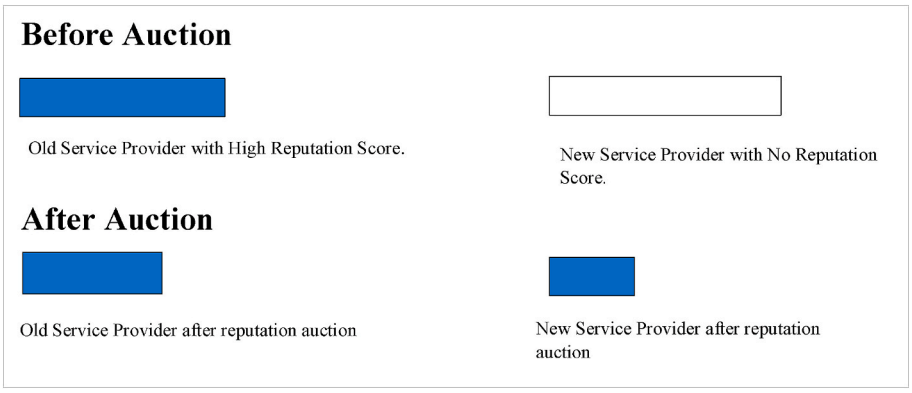

Fig. 7. Example of reputation scores before and after the auction.

reputation score is commercial. As long as they are building their reputation score by providing good services and products, their customers will rate them with a high rating. The providers can use this as a new source of income thus making the reputation score an important matter in the market. Fig. 7 shows an example of reputation scores before and after the auction.

5.4. Detection of non-compliant behavior (Req: 4)

The smart contract needs to have validated methods of detecting and dealing with any reputation fraud. This is the most critical part of the smart contract. To achieve this, the smart contract needs to be evaluated from time to time by deploying the Ethereum Ropsten network. The Metamask plugin can be installed first so that it communicates with nodes on the remote server. After switching to the Ropsten network, a new account can be created, and the solidity compiler is used to deploy the contract. The contract is then tested to detect any non-compliant behavior using the provided interface. Phase 2 of the FarMed framework in Fig. 4 represents the solution to this requirement and more information about it is provided in Fig. 5.

5.5. Mathematical models and algorithms (Req: 5)

To effectively compute the reputation values of service providers, generally and contextually as well as to enable reputation transfer, different mathematical models and algorithms mentioned earlier will be developed in this requirement. For the overall reputation computation, five-star algorithm will be used, for reputation computation in a specific context, a AKTiveRank algorithm will be used, and for reputation transfer, the EigenTrust algorithm will be used.

6. Conclusion and future work

This systematic literature review provides five key requirements that should be in a smart contract. Such requirements include the ability to derive reputation values and trust values of service providers based on the values present in the smart contracts and blocks respectively. Others include treating the reputation system as a digital asset and the detection of non-compliant behavior. After a thorough review of the existing literature, this paper proposed FarMed Service as a smart contract-based reputation system framework. This framework will address all the key requirements of smart contracts.

This SLR does not claim to have exhausted the entire literature search on the subject. It represents the first attempt to address the issues observed in blockchain-based reputation systems using smart contracts. It also represents the only approach of its type that proposes innovative artificial intelligence (AI)-based algorithmics on top of blockchain to carry out reliable trust and reputation computations, deduce reputation values of service providers and carry out context-based trust assessments for service providers. In future work, we intend to implement the different phases of FarMed framework and include the provision of an intelligent framework that executes an Ethereum smart contract-based reputation system in the blockchain network. Reputation systems should be able to support many users, ensure the integrity of the ratings or trust scores, and provide reliable mechanisms to support new users to bootstrap into the reputation-based economy. These too will be investigated and implemented in our future work.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Al-Bassam, M., 2017. SCPKI: a smart contract-based PKI and identity system. In: Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts. ACM, pp. 35–40.
Alani, H., Brewster, C., 2006. Metrics for Ranking Ontologies. *Intelligence, Agents. Multimedia Group,* School of Electronics and Computer Science University of Southampton Southampton, UK.
Angles, R., Gutierrez, C., 2005. Querying rdf data from a graph database perspective. In: Proc. Of 2nd European Semantic Web Conference. Crete, pp. 346–360. ESWC.
Atzori, M., 2016. Blockchain Technology and Decentralized Governance: Is the State Still Necessary? (Available at: SSRN).
Audun, J., Roslan, I., Colin, B., 2007. A Survey of Trust and Reputation Systems for Online Service Provision. Information Security Research Centre Queensland University of Technology, Brisbane, Australia.
Bigi, G., Bracciali, A., Meacci, G., Tuosto, E., 2015. Validation of decentralised smart contracts through game theory and formal methods. In: Programming Languages with Applications to Biology and Security. Springer, pp. 142–161.
Buterin, V., 2014. A Next-Generation Smart Contract and Decentralized Application Platform. White Paper.
Caesar, C., 2018. How to Build a Reputation System on Blockchain?' Bitconch White Paper Gives Out a Great Answer.
Cai, Y., Zhu, D., 2016. Fraud Detections for Online Businesses: a Perspective from Blockchain Technology (Financial Innovation).
Casassa, M., Tomasi, M., Montanari, L., 2001. An Adaptive System Responsive to Trust Assessment Based on Peer-To-Peer Evidence Replication and Storage. Hewlett Packard Laboratories. Technical report HPL-2001-133.
Christidis, K., Devetsikiotis, M., 2016. Blockchains and smart contracts for the internet of things. IEEE Access 4, 2292–2303.
Cong, L.W., He, Z., 2018. Blockchain Disruption and Smart Contracts (No. W24399). National Bureau of Economic Research.
Delmolino, K., Arnett, M., Kosba, A., Miller, A., Shi, E., 2016. Step by step towards creating a safe smart contract: lessons and insights from a cryptocurrency lab. In: International Conference on Financial Cryptography and Data Security. Springer, Berlin, pp. 79–94.
Dennis, R., Owenson, G., Aziz, B., 2016. A temporal blockchain: a formal analysis. In: International Conference on Collaboration Technologies and Systems (CTS). IEEE, pp. 430–437.
English, M., Auer, S., Domingue, J., 2016. Block chain technologies & the semantic web: a framework for symbiotic development. In: Lehmann, J., Thakkar, H., Halilaj, L., Asmat, R. (Eds.), Computer Science Conference for University of Bonn Students, pp. 47–61.

Fensel, D., Harmelen, F., Klein, M., Akkermans, H., Kidd, I., 2000. On-ToKnowledge: ontology-based tools for knowledge management,". In: The eBusiness and eWork 2000 Conference (EMMSEC 2000). Cheshire Henbury, E Madrid.
Frantz, C.K., Nowostawski, M., 2016. From Institutions to Code: towards Automated Generation of Smart Contracts. IEEE International Workshops on Foundations and Applications of Self Systems, pp. 210–215.
Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., Santamaría, V., 2018. Blockchain and smart contracts for insurance: is the technology mature enough? Future Internet 10 (2), 20.
Gomez-Perez, A., Corcho, O., 2002. "Ontology specification languages for the semantic web,". IEEE Intell. Syst. 17, 54–60.
Hendrikx, F., Bubendorfer, K., Chard, R., 2015. Reputation systems: a survey and taxonomy. J. Parallel Distr. Comput. 75, 184–197.
Idelberger, F., Governatori, G., Riveret, R., Sartor, G., 2016. Evaluation of logic-based smart contracts for blockchain systems. In: International Symposium on Rules and Rule Markup Languages for the Semantic Web. Springer, pp. 167–183.
Josang, A., Ismail, R., Boyd, C., 2007. A survey of trust and reputation systems for online service provision. Decis. Support Syst. 43 (2), 618–644. March.
Khan, A., 2015. Bitcoin – payment method or fraud prevention tool? Comput. Fraud Secur. 2015 (Issue 5), 16–19. (Accessed May 2015).
Khaqqi, K.N., Sikorski, J.J., Hadinoto, K., Kraft, M., 2018. Incorporating seller/buyer reputation-based system in blockchain-enabled emission trading application. Appl. Energy 209 (January), 8–19.
Kosba, A., Miller, A., Shi, E., Wen, Z., Papamanthou, C., 2016. Hawk: the blockchain model of cryptography and privacy-preserving smart contracts. IEEE Symp. Secur. Priv. 839–858.
Lauslahti, K., Mattila, J., Seppala, T., 2017. Smart Contracts–How Will Blockchain Technology Affect Contractual Practices?, vol. 68 ETLA Reports No.
Marino, B., Juels, A., 2016. Setting standards for altering and undoing smart contracts. In: International Symposium on Rules and Rule Markup Languages for the Semantic Web. Springer, Cham, pp. 151–166.
Resnick, P., Zeckhauser, R., 2015. Trust among strangers in internet transactions: empirical analysis of eBay' s reputation system. In: Economics of the Internet and E-Commerce.
Schaub, A., Bazin, R., Hasan, O., Brunie, L., 2016. A trustless privacy-preserving reputation system. In: IFIP International Information Security and Privacy Conference. Springer, Cham, pp. 398–411.
Sherman, L., 2018. A Decentralized Reputation System. How Blockchain Can Restore Trust In Online Markets.
Soska, K., Kwon, A., Christin, N., Devadas, S., 2016. Beaver: A Decentralized Anonymous Marketplace with Secure Reputation. IACR Cryptology ePrint Archive, p. 464.
Tadelis, S., 2016. Reputation and feedback systems in online platform markets. Annual Review of Economics 8, 321–340.
Tonelli, R., Destefanis, G., Marchesi, M., Ortu, M., 2018. Smart Contracts Software Metrics: a First Study. Elsevier arXiv preprint arXiv:1802.01517.
Watanabe, H., Fujimura, S., Nakadaira, A., Miyazaki, Y., Akutsu, A., Kishigami, J., 2016. Blockchain contract: securing a blockchain applied to smart contracts. In: IEEE International Conference on Consumer Electronics (ICCE), pp. 467–468.
Wohrer, M., Zdun, U., 2018. Smart contracts: security patterns in the ethereum ecosystem and solidity. In: 2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE), IEEE, pp. 2–8.
Wood, G., 2014. Ethereum: a secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper 151, 1–32.
Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., et al., 2017. A taxonomy of blockchain-based systems for architecture design. In: 2017 IEEE International Conference on Software Architecture (ICSA), pp. 243–252.
Zyskind, G., Nathan, O., 2015. Decentralizing Privacy: Using Blockchain to Protect Personal Data', Security and *Privacy Workshops (SPW)*. IEEE, pp. 180–184.

Ahmed Al Masoud is a postgraduate research student at the Faculty of Engineering and Information Technology, University of Sydney. His key research interests are in trust-based computing, Blockchain, Smart Contracts.

Dr Farookh Khadeer Hussain is an Associate Professor in School of Software, University of Technology Sydney. He is an Associate Member of the Advanced Analytics Institute and a Core Member of the Centre for Artificial Intelligence. His key research interests are in trust-based computing, cloud of things, blockchains and machine learning. He has published widely in these areas in top journals such as FGCS, The Computer Journal, JCSS, IEEE Transactions on Industrial Informatics, IEEE Transactions on Industrial Electronics etc.

Dr Omar Hussain is an Associate Professor at the University of New South Wales, Canberra. His research interests are in business intelligence, cloud computing and logistics informatics. In these areas, his research work focusses on utilizing decision making techniques for facilitating smart achievement of business outcomes. His research work has been published in various top international journals such as Information Systems, The Computer Journal, Knowledge Based Systems, Future Generation of Computer Systems etc. He has won awards and funding from competitive bodies such as the Australian Research Council for his research.