Strengthening the Blockchain-based Internet of Value with Trust

Nguyen B. Truong*, Tai-Won Um†, Bo Zhou*, Gyu Myoung Lee*
* Department of Computer Science, Liverpool John Moores University, Liverpool, L3 3AF, UK
Email: {n.b.truong@2015., b.zhou@, g.m.lee@}ljmu.ac.uk
† Department of Information and Communication Engineering, Chosun University, Gwangju, Korea
Email: twum@chosun.ac.kr

***Abstract*—In recent years, Blockchain has been expected to create a secure mechanism for exchanging not only for cryptocurrency but also for other types of assets without the need for a powerful and trusted third-party. This could enable a new era of the Internet usage called the Internet of Value (IoV) in which any types of assets such as intellectual and digital properties, equity and wealth can be digitized and transferred in an automated, secure, and convenient manner. In the IoV, Blockchain is used to guarantee the immutability of transactions meaning that it is impractical to retract once a transaction is confirmed. Therefore, to strengthen the IoV, before making any transactions it is crucial to evaluate trust between participants for reducing the risk of dealing with malicious peers. In this article, we clarify the concept of IoV and propose a trust-based IoV model including a system architecture, components and features. Then, we present a trust platform in the IoV considering two concepts, Experience and Reputation, originated from Social Networks for evaluating trust between two any peers in the IoV. The Experience and Reputation are characterized and calculated using mathematical models with analysis and simulation in the IoV environment. We believe this paper consolidates the understandings about IoV technologies and demonstrates how trust is evaluated and used to strengthen the IoV. It also opens important research directions on both IoV and trust in the future.**

***Index Terms*—Trust; Blockchain; Smart Contract; Internet of Value; Feedback; REK Trust Model; Experience; Reputation**

I. Introduction

The turn of the last century brought us to the Internet of Things (IoT) in which billions of devices are interconnected producing massive amount of data every second. There will be approximately 5,200GB of data for every person on Earth, and the size of the *'Digital Universe'* will reach to 44ZB (i.e., 44 trillion GB)[1]. The current Internet infrastructure enables us to send general information such as photos, text, audio and video files on your local computers to others at reasonable speed. How about in the future? Imagine that you are living in a smart home equipped with variety of sensors and personal gadgets producing huge amount of data every day. The question is that: will data transactions be operated in the same manner as we are currently exchanging information on the Internet? We believe that it should not be. The first reason is that it is not suitable for exchanging vast amount of data across the network which incurs much overhead and can cause severely damage to the IoT infrastructure. This issue can be overcome by interchanging the ownerships only, but not the data itself; then counterparts just need to get the data from cloud storage. Here, the data ownerships, used as a mean of exchange, are digital values representing the actual data. In this manner, various types of assets such as software programs, songs, pictures, and real-estates can be transacted in the same manner exchanging the represented value [1]. The second reason is that the current data exchange model is facing a problem called *'double spend'*. That is when a person sends her data to others, she is not actually sending the data, but she is sending its copy. Therefore same data can be sold many times. The *'double spend'* problem can be overcome by using a trustworthy (and powerful) intermediary for controlling the exchange [2]. The intermediary guarantees that assets will be securely and safely transferred and settled. However, the involvement of such third-parties in value exchange imposes delay in processing and single-point failure, introduces terrific threats and risks, and more importantly, comes at a cost. Fortunately, these are what Blockchain naturally deals with [3]. Blockchain is expected to have a huge impact on how people exchange their assets (both physical and digital ones) by enabling peer-to-peer (P2P) transactions of value in a secure manner while tackling down the *'double spend'* problem without the introduce of a intermediary.

From the two reasons and the prospective solutions for the data exchange example above, a novel paradigm Internet of Value (IoV) is generalized and coined. The IoV is as a platform of the next generation Internet that enables various types of assets to be digitized and represented as digital values, and directly and securely exchanged using Blockchain. Recently, several speeches from industrial companies such as TED[2] and Ripple Labs[3] have mentioned the term IoV and its provisioning. To the best of our knowledge, this paper is the first academic article dedicated to develop IoV technologies. In this paper, regarding to IoV environment, two terminologies *'user'* and *'entity'* are used interchangeably.

In the IoV, Blockchain is used for implementing transactions of value, consequently security, integrity, and non-

[1]The source can be found in https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm

[2]https://www.ted.com/talks/rachel_botsman_the_currency_of_the_new_economy_is_trust

[3]https://ripple.com/insights/chris-larsen-on-the-internet-of-value

reputability of the transactions are assured. However, once a transaction is verified and posted to Blockchain, it is greatly challenged to revert. Therefore, in order to prevent frauds, there should be a mechanism to evaluate trust relationship between an entity and counterparts that the entity is going to deal with before making any transactions. In this regard, a trust evaluation platform is critical for empowering and strengthening the IoV. In this article, we firstly present the concept of the IoV along with a conceptual system model; then focus on developing a trust platform for the IoV leveraging the Reputation-Experience-Knowledge (REK) trust model [4], [5]. Here, the two trust indicators (TIs) called Experience and Reputation are calculated based on the information in transactions (i.e., interactions) between entities in the IoV that are recorded in Blockchain. After each interaction, a trustor is more aware of its trustees based on how well the trustees has completed the transaction; and with an appropriate evaluation model, the Experience between the two entities is established and maintained. Moreover, by utilizing a Blockchain-based feedback mechanism, Experience between IoV entities can be securely recorded and shared throughout the IoV network; consequently, Reputation for any entity can be obtained by considering all Experience toward that entity as well as the IoV network topology. As a result, trust relationship between any two entities in IoV can be evaluated by combining Experience and Reputation. The main contributions of in this paper are three-fold:

- Introduce the concept and provisioning of the IoV considering Blockchain technology.
- Propose a conceptual trust-based IoV model consisting of the system operations, the reference architecture and components.
- Propose a trust platform based on Experience and Reputation concepts utilizing the REK trust model [4] for evaluating trust between two entities in the IoV.

The rest of the paper is organized as follows. Section II clarifies the concept and provisioning of the IoV with background knowledge. Section III presents the conceptual trust-based IoV model. The following section introduces the trust evaluation mechanism including Experience and Reputation computational models. Section V concludes our work and outlines future research directions.

II. Internet of Value: Background and Concept

A. The Blockchain-based IoV: Concept Clarification and Provisioning

To understand the concept of IoV, we start by explaining (distributed) cryptocurrencies. A cryptocurrency is a digital asset serving as a means of exchange accepted by participants in a transaction. Cryptocurrencies are not necessarily issued by a public authority or a bank, instead, they use distributed digital cryptography protocols to securely manage the creation and the transactions of the currencies [6]. In this regard, cryptocurrencies can be considered as a type of digital asset represented by digital value in the IoV. Bitcoin was the first cryptocurrency introduced in 2009 and remains the largest in terms of market capitalization. Besides, numerous cryptocurrencies have been created as blends of Bitcoin alternatives. Bitcoin and its derivatives are deployed in a distributed manner using Blockchain technology as a role of a distributed ledger. Such cryptocurrencies provide some key benefits that traditional currencies cannot offer. For example, verification and settlement of payment can be done in seconds (or minutes) regardless of geographical distance. There is no exchange rate, no intermediate fee, and just a low cost of transaction verification because transactions are done directly without the need for a third-party service provider [7]. The *'double spend'* problem is also completely eliminated by Blockchain native characteristic through miner verification of proof-of-work (PoW) process [8].

Bitcoin and other crypto-protocols are one of the most interesting cutting edges in payments industry, however, beyond that, the true enormous buzz is that transactions of various types of assets, not only the cryptocurrencies, could be manipulated based on the Blockchain technology. That is a Blockchain-based Value Exchange could be incorporated for asset exchanges such as *'physical and digital properties, equities, bonds, Artificial Intelligence (AI), and an enormous wave of applications which have not yet been conceived'* [9]. This is the initial idea of the IoV concept.

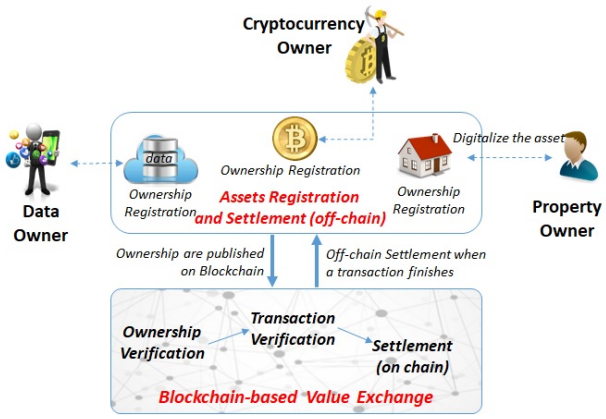

Fig. 1: IoV model for asset exchange using Blockchain-based Value Exchange layer

As illustrated in Fig. 1, the conceptual IoV model requires two main components to be built: (i) the Assets Registration and Settlement and (ii) the Blockchain-based Value Exchange. The first component is related to business and management that is out the scope of this paper. We mainly focus on developing the second component that recently has attracted a large number of government institutions and private companies. It is provisioned to be an additional component in the IoT for value exchanges. To do so, besides the Blockchain technology that provides mechanisms for securing value transactions, the concept of Smart Contract is also introduced as an agreement with terms and conditions between the participants in a transaction. Smart Contracts are in form of logics (computer code) and are accomplished and recorded on top of the Blockchain-based Value Exchange [10].

B. Blockchain Technology

Blockchain is a distributed immutable database that consists of a continuous growing list of blocks. Each block consists of two parts: *'a header'* that contains a timestamp, a unique ID (i.e., the hash of the Merkle tree), and the ID of the prior block; and a *'data part'* that is the record of one or more transactions between peers in a network. Thus, a corresponding block links with its previous block by appending the ID of the previous block in the header, hence the name Blockchain. Transactions are encrypted using mathematical algorithms and need to be verified (i.e., be signed) for validity before being hashed and encoded into a Merkle tree whose root is the hash of the corresponding block [11].

A transaction using Blockchain is verified if and only if more than 50% nodes in the Blockchain network reach consensus about its validity (the principle of Longest Chain Wins) [3]. Once verified, the transaction will be appended in an existing chain of blocks, synchronized and distributed across the network, thus, every node in the network has exactly the same copy of the database. This is why Blockchain is considered as an open, distributed ledger. By nature, Blockchain is inherently resistant to data modification. Once recorded, data in any given block cannot be altered retroactively as this would invalidate all hashes in the previous blocks in the Blockchain. The only way to modify a stored transaction in chain is to alter all subsequent blocks located in more than 50% of computers in the network, which is greatly challenged [12]. Consequently Blockchain technology opens a new type of distributed ledger for recording transactions securely and efficiently. The ledger can also be programmed using Smart Contracts in order to verify, audit and trigger transactions in an inexpensive, consistent and automatic manner [13]. Recently, Blockchain with Smart Contracts have been provisioning to be key technologies to create a secure platform for directly exchanging not only digital money but also various kinds of assets including intellectual property, rights and wealth [14].

C. Smart Contracts

Smart Contracts are agreements between the participants of a transaction, written in a Turing-complete programming language, for exchanging assets [10]. Smart Contracts are written onto Blockchain for extending the semantics of transactions. Indeed, Bitcoin transactions use a simple form of Smart Contracts that only define sender address, receiver address and amount of Bitcoin to be transferred leveraging the use of private and public keys. In the IoV, Smart Contracts are decentralized arbitrary performed upon the Blockchain-based Value Exchange. This is different from traditional centralized arbitrary e-systems which are based on central contract systems. As an agreement established by the parties involved, a Smart Contract consists of terms and conditions written in machine code to implement complex business rules. The terms in a Smart Contract dictate movement of value based on conditions met. For example, on a specific date (i.e., condition), the ownership of the data is changed from the data owner to the data buyer; in exchange, some amount of Bitcoin is transferred from the data buyer to the data owner. The use of Blockchain is to create a distributed, immutable storage; whereas the use of Smart Contracts brings a distributed, immutable escrow. This sets the IoV apart from the current Blockchain-based applications.

III. Toward a Trust-based IoV Platform

Trust is the underlying psychological measurement of an entity (i.e., the trustor) indicating whether it should put itself into a risky situation in case a trustee turns out to be misplaced. Blockchain is the driving force behind the IoV that assures security, integrity, and non-reputability of value transactions; and, trust plays a crucial roles in empowering the IoV. The use of trust in the IoV is two-fold: (i) to help evaluating assets; and (ii) to prevent frauds as well as encourage transactions in the IoV by providing trust evaluation between participants before making any transactions. This section proposes a conceptual trust-based system model with Blockchain for the IoV.

A. Trust-based IoV System Procedure

The procedure for exchanging value in the trust-based IoV platform is described in Fig. 2. The procedure consist of four major steps in an IoV transaction: (1), (2), (3), (4-1) and (4-2). The Smart Contract establishment (1) is conducted at the IoV Apps & Services before posting it to the Blockchain. After that, the steps (2), (3) and (4-1) are the native functions of Smart Contracts and Blockchain. The two trust-related components called Trust Evaluation and Value Evaluation are also introduced in the IoV platform.

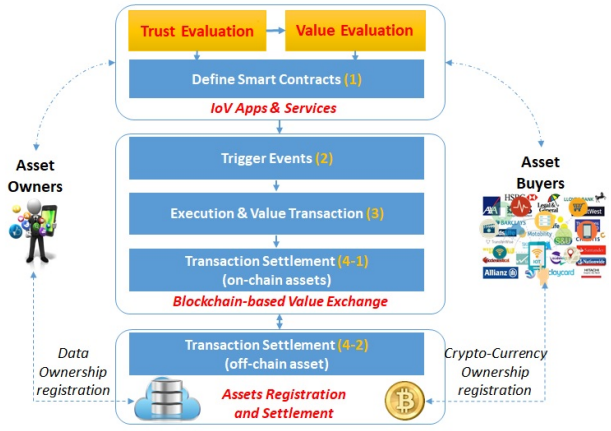

Fig. 2: Conceptual Platform and Procedure for Value Exchanges in Trust-based IoV

The Trust Evaluation component is to support transactions with trustworthy counterparts. That is, users base on trust to decide whether they should exchange assets with unknown counterparts without any trusted third-parties in IoV because once a transaction is settled, it is impossible to retract. This means that a user need to have a clue of *'belief'* or *'assurance'* of its counterparts before making any decision to transact with. The below pseudo-code illustrates a Smart Contract that leverages trust as a trigger event to automatically withdraw risky transactions.

```
event Checking(Address trustor, Address trustee, float threshold);

function trust_check(Address trustor, Address trustee, float threshold) {
        if (trust_evaluation(trustor, trustee) < threshold return 0;
        transaction(trustor, trustee);
}
```

The Value Evaluation component, as a part of the Service and Application Support layer, helps evaluating value for assets to be exchanged (Fig. 3). And, the Trust Evaluation component plays an important role in value evaluation of an asset due to the fact that value of an asset is high when the owner of the asset is trustworthy and vice versa. The trust-based value evaluation for assets is one of the future research direction on the IoV.

B. IoV Reference Architecture Aligned with IoT

The proposed IoV architecture is aligned with the ITU-T IoT and Smart Cities & Communities reference model[4]. The additional components namely Trust, Value Evaluation, Asset Registration, and Blockchain-based Value Exchange layer are introduced and aligned with the IoT components in the architecture (Fig. 3).

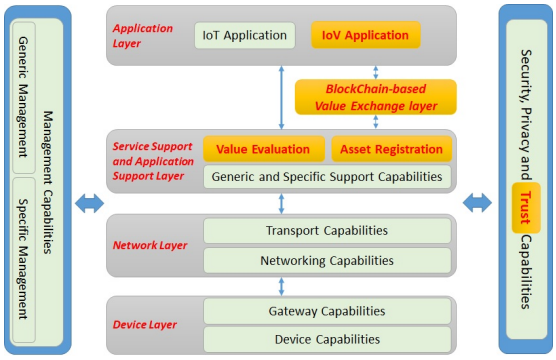

Fig. 3: IoV High Level Architecture (HLA) Functional Model

The Blockchain-based Value Exchange layer is located between Application layer and Service Support and Application Support layer whereas Value Evaluation and Asset Registration components belong to the Service Support and Application Support layer. The Trust component (with Security and Privacy components) is a multi-level capability interacting with all IoT layers, from the Device to the Application layers.

C. Feedback Mechanism

In order to establish and evaluate trust in the IoV, a feedback mechanism is deployed for gathering information about participants after each transaction. When a transaction is completed, the feedback mechanism enables participants to give opinions on how their counterparts have done to fulfill the transaction. The feedback value is personally evaluated based on how each entity perceives the effects after the transaction. Feedback can be both implicit and explicit; and may or may not requires human participation [15]. Different scenarios in the IoV have different feedback evaluation methodologies. There are two main techniques for valuating feedback. The first technique asks for users to give opinions after a transaction finishes which depends completely on human participants. This approach usually requires huge effort to engage users; and opinions are sometimes biased. This technique has been used in many e-commerce services and reputation systems such as eBay, Amazon and Airbnb. The second method valuates feedback based on calculation models that does not require human participation. For example, Quality of Data (QoD) [16] can be used as the valuation of feedback for data exchange in the IoV.

Feedback can also use Blockchain (along with the Blockchain for transactions). Each feedback consists of a source (i.e., entity ID that gives feedback), a destination (i.e., target entity ID), value, and timestamp when a transaction is verified. The trust platform then looks for this information in the feedback Blockchain to calculate the Experience and Reputation for inferring final trust values. There should be an important assumption that the IoV platform should deploy an identification mechanism for all of its entities. And the feedback Blockchain is then based on advanced Byzantine Fault-Tolerant (BFT) state-machine replication protocols which require IDs for all users in the IoV network [17]. This type of Blockchain is different from the conventional proof-of-work consensus technique called *'permissionless Blockchain'* implemented in Bitcoin in which participants are anonymous and transactions are conducted based on *'one-time' Bitcoin address*. Thus the drawback of our approach is the privacy preservation and it would be one of the challenges and future research directions.

IV. Trust Evaluation Mechanism

The REK model in the IoT environment are utilized for evaluating trust in the IoV. In the REK model, trust is comprised of the three Reputation, Experience and Knowledge indicators; however, in the IoV, there is not yet available information for quantifying the Knowledge. Instead, transactions between entities are recorded in Blockchain and distributed to peers in the IoV network, which is suitable for the Experience and Reputation calculations.

A. Experience Computational Model

Experience is a type of asymmetric relationship between two entities obtained from previous interactions between the two indicating to what extend a trustor trusts a trustee. To enable the Experience computational model, the feedback mechanism introduced in sub-section III.C is integrated as demonstrated in Fig. 4.

To model experience between two entities, we investigate and imitate human relationships in trust-related sociological literature [18], [19]. That is, Experience is increased due to cooperative feedback and is decreased by uncooperative feedback. Experience also decays if there is no interactions between the two. The increase, decrease and decay of Experience depend on the intensity of transactions, feedback value

[4]http://www.itu.int/en/ITU-T/studygroups/2017-2020/20/Pages/default.aspx

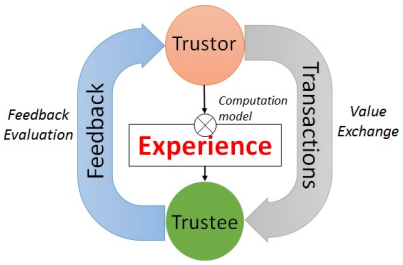

Fig. 4: Experience computation model based on feedback mechanism

ϑ, and the current Experience value Exp_t. Thus, Experience can be modeled using mathematical difference equations.

- **Increase (due to cooperative feedback)**

Let ϑ be the feedback value of a transaction, normalized in the range $(0, 1)$. Cooperative feedback means $\vartheta > \theta_{cooperative}$.The Increase trend is modeled using a linear difference equation as following:

$$Exp_{t+1} = Exp_t + \vartheta_t \times \Delta Exp_{t+1} \quad (1)$$

$$\Delta Exp_{t+1} = \alpha \times (1 - \frac{Exp_t}{max_{Exp}}) \quad (2)$$

where Exp_t, $init_{Exp}$, max_{Exp}, ϑ_t, α are the Experience value at the time t, the initial Experience value, the maximum value of Experience, the Cooperative feedback value at the time t, and the maximum increase value of Experience, respectively. Note that $0 < \vartheta_t < 1$ and $0 < \alpha < max_{Exp}$.

- **Decrease (due to uncooperative feedback)**

An uncooperative interaction means $\vartheta < \theta_{uncooperative}$. The Decrease trend is modeled as following:

$$Exp_{t+1} = Max(min_{Exp}, Exp_t - (1 - \vartheta_t) \times \beta \times \Delta Exp_{t+1}) \quad (3)$$

where ΔExp_{t+1} is determined by Equation (2); ϑ_t, $\beta > 1$ and min_{Exp} are the uncooperative feedback value at the time t, the Decrease rate and the minimum Experience value, respectively.

- **Decay (due to neutral feedback or no interaction)**

In sociology, relationship between people decays over time if participants do not interact, although the decay rates are different depending on strength of the current relationships [20]. Strong relationships tend to exhibit less decay than the weak ones, and the decay value is assumed to be inversely proportional to current relationship value. Similarly, Experience decays due to no transaction after a period of time or due to neutral feedback (i.e., $\theta_{uncooperative} \leq \vartheta \leq \theta_{cooperative}$). The mathematical Decay model is as following:

$$Exp_{t+1} = Max(init_{Exp}, Exp_t - \Delta decay_{t+1}) \quad (4)$$

$$\Delta decay_{t+1} = \delta(1 + \gamma - \frac{Exp_{t-1}}{max_{Exp}}) \quad (5)$$

where δ and γ are the minimal decay value and the decay rate, respectively.

The simulation for the Experience model is conducted in Matlab with the parameters are shown in Table I and the results

TABLE I: PARAMETERS SETTINGS IN THE EXPERIENCE SIMULATION

Parameters	Values	Parameters	Values
max_{Exp}	1	γ	0.005
min_{Exp}	0	δ	0.005
$init_{Exp}$	0.3	$\theta_{uncooperative}$	0.3
α	0.1	$\theta_{cooperative}$	0.6
β	2	ϑ	(0, 1)

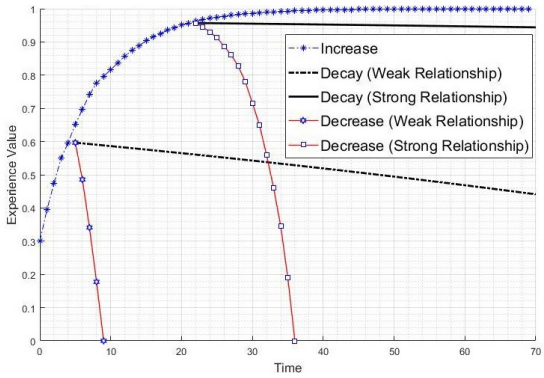

Fig. 5: Experience Model consists of Increase, Decrease and Decay trends

are illustrated in Fig. 5. Note that different use-cases might result in different parameter settings. Generally, in both human society and the IoV, high Experience value indicates a strong relationship between the two and vice versa.

According to the Increase trend model and the simulation result depicted in Fig. 5, Experience accumulates from cooperative feedback and the accumulated value depends on both feedback value and the current Experience value. It requires more and more cooperative interactions in order to get higher Experience value, meaning that strong relationships are difficult to achieve. It is easy to prove that the Experience model forms a curve that is incremental and asymptotic to 1 (i.e., max_{Exp}). However, regarding to the Decrease model, these strong relationships are more resistant to uncooperative interactions whereas weak relationships are severely damaged (Fig. 5). The Decrease rate $\beta = 2$ means that Experience loses *twice* in case of an uncooperative interaction compared to what it has gained from a cooperative interaction. Similar to the Decrease model, strong relationships decay much slower than the weak ones (Fig. 5). Relationships between entities require periodic maintenance but strong ones tend to persist longer even without reinforcing cooperative interactions. This is similar to what happens in the human society, thus, the proposed Experience model effectively migrates the trust relationship in the real world to the IoV.

B. Reputation Computation Model

Reputation of an entity (regarding to the trust context) is a concept indicates a perception of society about the trustworthiness of this entity. The goal of any reputation systems is to provide an estimation of the trustworthiness, thus, encourages other entities to interact with this entity without first-hand knowledge. In the IoV, only small number of users that have already interacted with another, resulting in very high possibility that two any entities are new to each

other, consequently no experience between the two. Therefore, reputation is the important information in trust evaluation.

Unlike Experience is a subjective relationship, Reputation is an objective property of an entity. We follow the idea that Reputation of an entity in the IoV network is calculated based on both Experience and Reputation from/of the entities that have interacted with this entity. This is somewhat similar to the $GooglePageRank^{TM}$ algorithm [21] except that it is more complicated due to the consideration of weighted links between two entities. That is the links between two entities (i.e., Experience between the two) could be either supportive or unsupportive, resulting in increasing or decreasing of Reputation value, respectively. A novel mathematical model for Reputation is proposed as following:

$$Rep_{Pos}(X) = \frac{1-d}{N} + d(\sum_{\forall i} Rep_{Pos}(i) x \frac{Exp(i,X)}{C_{Pos}(i)}) \quad (6)$$

$$Rep_{Neg}(X) = \frac{1-d}{N} + d(\sum_{\forall i} Rep_{Neg}(i) x \frac{1-Exp(i,X)}{C_{Neg}(i)}) \quad (7)$$

$$Rep(X) = max(0, Rep_{Pos}(X) - Rep_{Neg}(X)) \quad (8)$$

- $Rep_{Pos}(i)$ is positive reputation of the entity i considering only supportive Experience.
- $C_{Pos}(i) = \sum_{Exp(i,j)>\theta} Exp(i,j)$ is the total values of all supportive Experience that the entity i currently interacts with.
- $Rep_{Neg}(i)$ is negative reputation of the entity i considering only unsupportive Experience.
- $C_{Neg}(i) = \sum_{Exp(i,j)<\theta} (1 - Exp(i,j))$ is total compliments of unsupportive Experience that the entity i is currently interacts with.
- $Rep(i)$ is the reputation of the entity i which is the combination of the positive and negative reputation.
- N is total numbers of entities in the IoV networks.
- $Exp(i,X)$ is the Experience from the entity i toward the entity X.
- $d = 0.85$ is the damping factor which was intensively investigated on the web-ranking.

C. Reputation Model Mathematical Analysis and Simulation

Both Equations (6) and (7) can be expressed in *Markov chains* of *random process* with the Rep_{Pos} and Rep_{Neg} vectors as the stationary distributions, respectively (i.e., Rep_{Pos} and Rep_{Neg} are vectors formed from positive reputation $Rep_{Pos}(i)$ and negative reputation $Rep_{Neg}(i)$ $\forall i = \overline{1,N}$). These Markov chains are random suffer models with random jumps; consequently these Markov chains are strongly connected. Therefore, the Rep_{Pos} and Rep_{Neg} vectors, which are the stationary distribution of the Markov chains, are existed and unique. Therefore the Reputation defined in Equation (8) is also existed and unique. Details of the mathematical proofs and analysis for the Reputation model can be found in [22].

Based on the computational model, Reputation of all entities in the IoV network can be calculated either algebraically or iteratively. The algebra traditional method to solve the matrix equations in (6) and (7) takes roughly N^3 operations that is not suitable for a huge network like the IoV. On the other hand, the iterative methods is much faster because the Rep_{Pos} and Rep_{Neg} vectors calculations converge after conducting a number of iterations. Fig. 6 depicts the convergence rate for several network sizes $N = 1000, 2000$ and 4000 with the *error_tolerance* = 10^{-3}, which is the $2-norm$ vector of the difference between Rep vectors in two consecutive iterations.

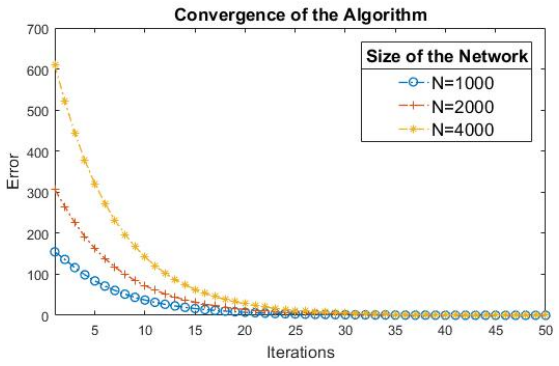

Fig. 6: Convergence of the Reputation algorithm with several network sizes

As can be seen from Fig. 6, the Reputation model converges to a reasonable tolerance (i.e., 10^{-3}) in less than 45 iterations. The convergences on half and one fourth of the data take 37 and 32 iterations, respectively. This graph suggests that this reputation model will well scale for a large network size as the scaling factor is roughly linear in $logN$. Therefore, the reputation model is suitable to deploy in a huge network like the IoV.

D. Finalize Trust Value

The final trust value is a composite of both Reputation and Experience. For example, a simple weighted sum for calculating trust value between A (i.e., the trustor) and B (i.e., the trustee) is as following:

$$Trust(A,B) = \alpha Rep(B) + \beta Exp(A,B) \quad (9)$$

where $\alpha > 0$ and $\beta > 0$ are weighting factors satisfying $\alpha + \beta = 1$. The weighting factors can be autonomously adjusted using a machine learning mechanism that learns from feedback.

V. Conclusion and Future Work

In this paper, we have provided a comprehensive concept, system model and architecture for the IoV with Blockchain and Smart Contracts for a secure and distributed value exchange network. Beyond that, we have incorporated a trust platform for strengthening and empowering the trust-based IoV by utilizing the REK trust model in [4], [5]. The trust evaluation system in the IoV leverages a Blockchain-based feedback mechanism for gathering opinions about entities involved in IoV transactions that are already recorded in Blockchain. The Experience and Reputation computational models are then carried out based on the information from the feedback Blockchain. The two Reputation and Experience

models are simulated and analyzed for showing the effectiveness in quantifying trust in the IoV environment.

This paper is as a catalyst for IoV and trust-based IoV research that opens variety of future work. The first direction is to investigate and develop IoV components such as Blockchain-based Value Exchange layer, the Asset Registry and the Smart Contracts. Related to trust, one direction can be a novel trust evaluation model considering more information about IoV entities than only feedback. Another direction is the adaptation of the Experience and Reputation models which requires to adapt with parameters settings in a context-aware manner. The forth direction could be a mechanism for Value Evaluation component for a specific use-case that takes other factors, including trust, into account when judging asset value. We expect that our proposals can significantly contribute to further research activities in the future, taking into account Blockchain and trust issues for the IoV.

ACKNOWLEDGMENT

This work was supported by Institute for Information & Communications Technology Promotion (IITP) grant funded by the Korea government (MSIT). [2015-0-00533, Development of TII (Trusted Information Infrastructure) S/W Framework for Realizing Trustworthy IoT Eco-system] and the EU funded Horizon 2020 Wise-IoT project [The EC Grant Agreement No. 723156, Worldwide Interoperability for Semantics IoT].

REFERENCES

[1] J. Manyika, M. Chui, P. Bisson, J. Woetzel, R. Dobbs, and D. Ahua, "Unlocking the potential of the internet of things," *McKinsey Global Institute*, 2015.

[2] D. O'mahony, M. Peirce, and H. Tewari, *Electronic payment systems*. Artech House Norwood, 1997.

[3] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[4] N. B. Truong, H. Lee, B. Askwith, and G. M. Lee, "Toward a trust evaluation mechanism in the social internet of things," *Sensors*, vol. 17, no. 6, p. 1346, 2017.

[5] N. B. Truong, Q. H. Cao, T.-W. Um, and G. M. Lee, "Leverage a trust service platform for data usage control in smart city," in *Global Communications Conference (IEEE GLOBECOM)*, 2016.

[6] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press, 2016.

[7] R. Böhme, N. Christin, B. Edelman, and T. Moore, "Bitcoin: Economics, technology, and governance," *The Journal of Economic Perspectives*, vol. 29, no. 2, pp. 213–238, 2015.

[8] G. O. Karame, E. Androulaki, and S. Capkun, "Double-spending fast payments in bitcoin," in *Proceedings of the 2012 ACM conference on Computer and communications security*. ACM, 2012, pp. 906–917.

[9] J. Brito and A. Castillo, *Bitcoin: A primer for policymakers*. Mercatus Center at George Mason University, 2013.

[10] V. Buterin *et al.*, "A next-generation smart contract and decentralized application platform," *white paper*, 2014.

[11] R. C. Merkle, "Protocols for public key cryptosystems," in *Security and Privacy, 1980 IEEE Symposium on*. IEEE, 1980, pp. 122–122.

[12] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, "Bitcoin-ng: A scalable blockchain protocol." in *NSDI*, 2016, pp. 45–59.

[13] M. Iansiti and K. R. Lakhani, "The truth about blockchain," *Harvard Business Review*, vol. 95, no. 1, pp. 118–127, 2017.

[14] M. Swan, *Blockchain: Blueprint for a new economy*. O'Reilly Media, Inc., 2015.

[15] C. Dellarocas, "The digitization of word of mouth: Promise and challenges of online feedback mechanisms," *Management science*, vol. 49, no. 10, pp. 1407–1424, 2003.

[16] L. L. Pipino, Y. W. Lee, and R. Y. Wang, "Data quality assessment," *Communications of the ACM*, vol. 45, no. 4, pp. 211–218, 2002.

[17] M. Vukolić, "The quest for scalable blockchain fabric: Proof-of-work vs. bft replication," in *International Workshop on Open Problems in Network Security*. Springer, 2015, pp. 112–125.

[18] R. F. Baumeister and M. R. Leary, "The need to belong: desire for interpersonal attachments as a fundamental human motivation." *Psychological bulletin*, vol. 117, no. 3, p. 497, 1995.

[19] D. L. Oswald, E. M. Clark, and C. M. Kelly, "Friendship maintenance: An analysis of individual and dyad behaviors," *Journal of Social and Clinical Psychology*, vol. 23, no. 3, pp. 413–441, 2004.

[20] S. G. Roberts, R. I. Dunbar, T. V. Pollet, and T. Kuppens, "Exploring variation in active network size: Constraints and ego characteristics," *Social Networks*, vol. 31, no. 2, pp. 138–146, 2009.

[21] S. Brin and L. Page, "Reprint of: The anatomy of a large-scale hypertextual web search engine," *Computer networks*, vol. 56, no. 18, pp. 3825–3833, 2012.

[22] N. B. Truong, T.-W. Um, B. Zhou, and G. M. Lee, "From personal experience to global reputation for trust evaluation in the social internet of things," to appear in Global Communications Conference (IEEE GLOBECOM), 2017.