Anonymous Reputation System for IIoT-Enabled Retail Marketing Atop PoS Blockchain

Dongxiao Liu, *Student Member, IEEE*, Amal Alahmadi, Jianbing Ni, *Member, IEEE*, Xiaodong Lin, *Fellow, IEEE*, and Xuemin (Sherman) Shen, *Fellow, IEEE*

***Abstract*—Industrial Internet of Things (IIoT) is revolutionizing the retail industry for manufacturers, suppliers, and retailers to improve operational efficiency and consumer experience. In IIoT-enabled retail marketing, reputation systems play a critical role to boost mutual trust among industrial entities and build consumer confidence. In this paper, we focus on reputation management in the consumer–retailer channel, where retailers can accumulate reputations from consumer feedbacks. To encourage consumers to post feedbacks without worrying about being tracked or retaliated, we propose an anonymous reputation system that preserves consumer identities and individual review confidentialities. To increase system transparency and reliability, we further exploit the tamper-proof nature and the distributed consensus mechanism of the blockchain technology. With system designs based on various cryptographic primitives and a Proof-of-Stake consensus protocol, our blockchain-based reputation system is more efficient to offer high levels of privacy guarantees compared with existing ones. Finally, we explore the implementation challenges of the blockchain-based architecture and present a proof-of-concept prototype system by Parity Ethereum. We measure the on/off-chain performance with the scalability discussion to demonstrate the feasibility of the proposed system.**

***Index Terms*—Anonymous reputation, blockchain, Industrial Internet-of-Things (IIoT), retail marketing.**

I. Introduction

INDUSTRIAL Internet-of-Things (IIoT) [1], which consists of a global network of smart objects, is reshaping and revolutionizing the retail industry [2]. In a global retail ecosystem, suppliers, manufactures, and retailers are adopting IIoT to improve manufacturing operational efficiency and reduce supply-chain management cost [3], [4]. Leveraged with cloud computing and big data technologies, IIoT is also envisioned to benefit the retail marketing that speaks to the needs of competitive market globalization and consumer demand diversification [3]. With the help of IIoT technology, retailers are able to collect massive feedbacks from various sources and devices, which can help them better manage their business. In particular, consumer feedbacks play a critical role for retailers to establish reputations among industrial partners and to build consumer confidence [5]. Specifically, consumers are allowed to leave feedbacks (usually a rating score and/or a review message) for their experiences with retailers [6]. These feedbacks accumulate over time and can be enumerated by other entities in the retail industry.

However, there are still some challenging issues that could hinder the development of a reliable retail reputation system. First, the process of leaving feedbacks may reveal much personal consumer information, which can be used to track and profile consumers [7]. Moreover, consumers may be reluctant and compelled while leaving a negative review to a specific retailer in the fear of related consequences [8]. Simply leveraging pseudonyms for rating anonymity cannot resolve this concern, which can suffer from de-anonymization attacks [9]. Second, current reputation systems mainly utilize a centralized marketplace that collects and accumulates consumer reviews. However, it has been evidenced that the current centralized marketplace may fail to keep their promise of a desired trust level because of the leak of private consumer information and the lack of system transparency [6].

There have been some research efforts on designing a reputation system that provides strong consumer anonymity guarantees [7], [8], [10], [11] without relying on a centralized marketplace [6], [12], [13]. Besides anonymity, reputation systems are required to resist to various attacks (such as self-rating and Sybil attacks [14]), which becomes more challenging in a decentralized marketplace [13]. However, the existing decentralized solutions for reputation systems provide insufficient system transparency, which is essential for the IIoT-enabled retail marketing due to the lack of mutual trust among the involved entities. To realize a more open and transparent reputation system, extensive research efforts have been directed to the design of a blockchain-based architecture [6], [12]. In their designs, blockchain serves as an immutable ledger, where the review generation and reputation accumulation process can be publicly verified and traced. The underlying consensus and incentive mechanisms of the blockchain technology also contribute to the boost of mutual trust among consumers and retailers. Although

Manuscript received August 29, 2018; revised December 12, 2018; accepted January 29, 2019. Date of publication February 12, 2019; date of current version June 12, 2019. Paper no. TII-18-2764. *(Corresponding author: Xiaodong Lin.)*

D. Liu, J. Ni, and X. Shen are with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Canada N2L 3G1, (e-mail: dongxiao.liu@uwaterloo.ca; jianbing.ni@uwaterloo.ca; sshen@uwaterloo.ca).

A. Alahmadi is with the Department of Physics and Computer Science, Wilfrid Laurier University, Waterloo, Canada N2L 3C5, (e-mail: alah6650@mylaurier.ca).

X. Lin is with the School of Computer Science, University of Guelph, Guelph Canada N1G 2W1, (e-mail: xlin08@uoguelph.ca).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TII.2019.2898900

1551-3203 © 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

Authorized licensed use limited to: University of Waterloo. Downloaded on July 26,2020 at 19:15:18 UTC from IEEE Xplore. Restrictions apply.

these attempts [6], [12] have exploited blockchain technologies for building up a promising reputation system, the proposed systems pay insufficient attention to the efficiency and scalability issues of the blockchain technology [15]. Moreover, implementation challenges of a blockchain-based architecture have not been well investigated.

In this paper, we propose an Anonymous Reputation System atop a Proof-of-Stake blockchain (ARS-PS). The proposed ARS-PS allows retailers to establish reputations by selling products to consumers, which is identical to the practical needs of a retail marketing platform. Meanwhile, the ARS-PS ensures that retailer reputation accumulation process is transparent to the public while providing strong anonymity to consumers. The contributions of this paper are summarized as follows.

1) We design an efficient and anonymous reputation system by leveraging a randomizable signature [7], [16] with non-interactive zero-knowledge proof technique [17], [18]. The proposed system preserves the identity and the individual review confidentiality of the consumer. Only the aggregated review statistics for retailers is revealed to the public.
2) We design a blockchain-based architecture that implements the proposed anonymous reputation system to improve system transparency. With the off-chain rating token generation phase, the proposed architecture reduces the on-chain storage and computation overhead. We further exploit the PoS consensus protocol in [19] by associating retailer reputation with the stake. Security analysis demonstrates the reliability of the proposed blockchain-based architecture.
3) We explore two implementation challenges of the blockchain-based architecture: First, the compatibility with the current blockchain platforms, and, second, the insufficient support for cryptographic primitives. We develop a proof-of-concept prototype system based on Ethereum Parity [20]. We build a testing blockchain network, and the experimental results demonstrate the efficiency and feasibility of the proposed ARS-PS.

The remainder of this paper is organized as follows. In Section II, we present related works. In Section III, the system model, security model, and design goals are presented. In Section IV, we present the building blocks in this paper. In Sections V and VI, we propose the anonymous reputation system and the efficient integration with a Proof-of-Stake (PoS) blockchain. We analyze the security of the proposed ARS-PS in Section VII and evaluate its performance in Section VIII. Finally, we conclude this paper in Section IX.

II. Related Work

Trust and reputation management is becoming prevalent for the success of a global retail marketing system [21], [22]. Extensive research efforts have been devoted to developing an anonymous reputation system for marketplaces [7], [8], [10], [11], [13]. Blomer *et al.* [11] proposed a reputation system based on group signature technique. Motivated by [11], Blomer *et al.* [7] proposed a feedback-driven reputation system with public linkability. The main goal of the proposed system [7] is to preserve consumer anonymity while preventing double review attack. However, the proposed scheme [7] did not consider purchase–purchase unlinkability for consumers due to the use of the same commitment message for an individual consumer. Bag *et al.* [23] proposed a personalized reputation system taking into consideration the trustworthiness of consumers. Bazin *et al.* [13] designed a feedback-driven reputation system with secure rating aggregations. RSA blind signatures and non-interactive zero-knowledge proofs were leveraged in [13] to achieve consumer anonymity. Zhai *et al.* [10] proposed a tracking-resistant anonymous reputation system by leveraging an anonymity provider with mix-net technology. However, the proposed scheme in [10] required much computation and communication overhead due to the use of verifiable shuffle operations. Azad *et al.* [8] utilized a homomorphic cryptographic system and non-interactive zero-knowledge proof to design a decentralized reputation system with individual rating score confidentiality. Moreover, the proposed schemes [7], [8], [10], [11], [23] provide insufficient system transparency, which makes them less suitable for the retail marketing environment due to the lack of mutual trust among the involved entities.

To build a more transparent marketplace, blockchain technologies have been exploited for reputation system construction [6], [12]. Schaub *et al.* [12] proposed a fully decentralized reputation system atop a public blockchain with blind signature to achieve consumer anonymity. Soska *et al.* [6] proposed an anonymous reputation system based on ring signature, which resulted in a linear overhead when generating the anonymous review proof. Moreover, the openness of a public blockchain and consumer anonymity may raise the concern of Sybil attacks. In summary, the existing literature for blockchain-based reputation systems has achieved a variety of properties such as anonymity, decentralization, conditional linkability, and system transparency. However, less attention has been directed to the efficiency and scalability issues of a blockchain-based architecture in [6] and [12]. At the same time, implementation challenges of a blockchain-based reputation system are not well investigated in the design of the system to achieve compatibility with existing blockchain platforms.

III. Problem Formulation

In this section, we formulate the system model, security model, and the design goals of this paper.

A. System Model

In Fig. 1, there are three entities in our system: 1) consumers, 2) retailers, and 3) an identity management entity (IDM).

1) *Consumer.* A consumer, uniquely identified by C_i, can make purchases from retailers and later leave a numeric rating score for the retailer.
2) *Retailer.* A retailer, uniquely identified by R_j, can sell products to consumers and establish reputations from consumer feedbacks. Retailers also act as stakeholders and collaboratively maintain a public leger (denoted as $\mathcal{L}$) based on a PoS consensus protocol [19].

Authorized licensed use limited to: University of Waterloo. Downloaded on July 26,2020 at 19:15:18 UTC from IEEE Xplore. Restrictions apply.

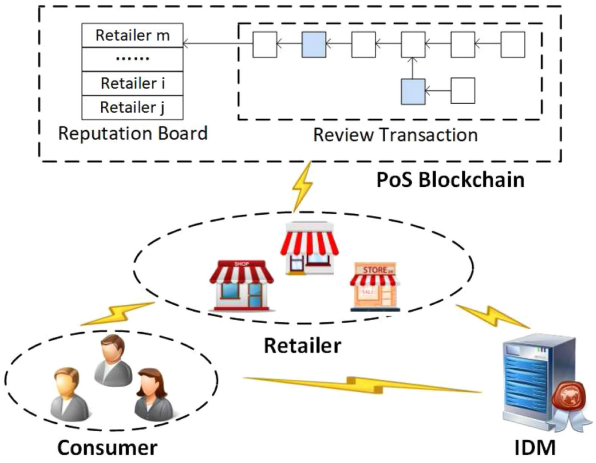


Fig. 1. System model.

3) *IDM*. It is a government agency that is in charge of issuing and managing identities and credentials of consumers and retailers.

At a high level, the ARS-PS works as follows. Consumers and retailers first register themselves to the IDM. Each consumer obtains an anonymous identity credential from the IDM. Afterward, consumers can make purchases from retailers and obtain an anonymous rating token. Later, a consumer can leave a review (a rating score) for a retailer by making a review transaction to $\mathcal{L}$ and privately tie the review to a previous purchase. Finally, the review transactions for the same retailer accumulate as a numeric score in the reputation board. Note that the IDM in the ARS-PS can be extended to a distributed identity management system [24].

B. Security Model

We assume the IDM to be fully trusted. This is reasonable since the IDM is a government agency responsible for the administration of citizens. Some consumers and retailers can be malicious and may launch a bunch of attacks to the system such as Sybil attacks, and white/bad mouthing attacks [7]. For the security of public leger $\mathcal{L}$, we borrow the assumptions from [19] and [25]. In particular, the stake in the PoS consensus protocol is associated with the reputation of retailers in the ARS-PS. We require that an adversary cannot control the majority of the stake (reputation) in the system. Meanwhile, we assume that a rational retailer (stakeholder) with high reputation (stake) is more willing to maintain the correctness of ledger $\mathcal{L}$. This is reasonable since the cost for a high-scored retailer to behave maliciously is huge [19].

C. Design Goals

Under the security assumptions, we summarize the design goals of the ARS-PS.

1) Bounded Confidentiality. A consumer's individual review statistics (rating scores) should be kept private. Only the aggregated retailer review statistics is to be revealed to the public. However, individual rating scores should have upper and lower boundaries. Consumers cannot submit rating scores that exceed the boundaries.
2) Conditional Anonymity. Obtaining a rating token or leaving a review on a public ledger will not expose a consumer's true identity. However, the IDM should be able to recover the true identity of an anonymous review in case of consumer misbehavior.
3) Unforgeability. The anonymous identity credential and rating token cannot be forged. Without the credential and the token, consumers cannot submit a valid review to the public ledger.
4) Confined Unlinkability. The public cannot determine if two valid reviews for different retailers are from the same consumer. However, the reviews are linkable if a consumer leaves multiple reviews for the same retailer.
5) Transparency. Review generation and reputation accumulation process should be transparent and publicly verifiable to all retailers and consumers.
6) Blockchain Security. The public transaction ledger should be robust, and on-chain transactions should be immutable.

IV. Building Blocks

In this section, building blocks in this paper are presented. We denote three cyclic groups, namely, $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{G}_T$, with a prime order p and a Type III bilinear pairing $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$. Also, $g, h \in \mathbb{G}_1$ and $\tilde{g} \in \mathbb{G}_2$ are generators of $\mathbb{G}_1$and$\mathbb{G}_2$. $\mathcal{H}$ is a collision-resistant hash function.

A. Zero-Knowledge Proof

The zero-knowledge proof technique enables one party (prover) to prove to another party (verifier) that she knows some secret s for a public verifiable relation without exposing the secrets. In this paper, we use the notation [26] for proof statement in the discrete-logarithm setting [27]. A typical example can be written as follows:

$$\mathbf{PK}\{(r_1, r_2) : Y_1 = h^{r_1} g^{r_2} \wedge Y_2 = g^{r_1}\} \tag{1}$$

where $r_1, r_2 \in \mathbb{Z}_p$ are the secrets that need to be proven, and $Y_1, Y_2, h, g \in \mathbb{G}_1$ are the public parameters. The above proof can be instantiated using sigma protocol with the Fiat–Shamir heuristic [17] as follows.

1) The prover chooses two random numbers $k_1, k_2 \in_R \mathbb{Z}_p$ and computes commitments $T_1 = h^{k_1} g^{k_2}$ and $T_2 = g^{k_1}$.
2) The prover computes $c = \mathcal{H}(Y_1, Y_2, T_1, T_2)$ and $z_1 = k_1 + cr_1$, $z_2 = k_2 + cr_2$.
3) For a given proof, T_1, T_2, z_1, z_2, the verifier computes $c = \mathcal{H}(Y_1, Y_2, T_1, T_2)$ and checks $T_1 \stackrel{?}{=} Y_1^{-c} h^{z_1} g^{z_2}$ and $T_2 \stackrel{?}{=} Y_2^{-c} g^{z_1}$. The verifier accepts the proof if all the conditions hold.

B. PS-Signature

Proposed by David Pointcheval and Olivier Sanders [16], [28], the PS-signature is a signature scheme with a short signature size. The secret parameter $\mathcal{S}$ for the signature scheme is

Authorized licensed use limited to: University of Waterloo. Downloaded on July 26,2020 at 19:15:18 UTC from IEEE Xplore. Restrictions apply.

x, y, where $x, y \in_R \mathbb{Z}_p$. The public parameter $\mathcal{P}$ is $(g, \tilde{g}, \tilde{X}, \tilde{Y})$, where $g \in \mathbb{G}_1, \tilde{g} \in \mathbb{G}_2$, and $\tilde{X} = \tilde{g}^x, \tilde{Y} = \tilde{g}^y$. PS-signature can be utilized to sign on committed messages, and the signature of the committed message is randomizable. In the following, two detailed techniques that are used to construct anonymous identity credentials and rating tokens are presented.

1) Sign on Committed Messages: We define a function $\text{SigCom}(T, \mathcal{P}, \mathcal{S}, u)$ that takes as input the commitment $T = g^m$ of a message $m \in \mathbb{Z}_p$, public/secret parameters $\mathcal{P}/\mathcal{S}$, and a random number $u \in_R \mathbb{Z}_p$. The function outputs σ as the PS-signature of the message m as follows:

$$\sigma = (\sigma_1, \sigma_2) = (g^u, (g^x \cdot T^y)^u). \tag{2}$$

2) Prove the Knowledge of a Signature: Suppose that we have a signature tuple $\sigma = (\sigma_1, \sigma_2)$ of a message m. The prover first chooses $t \in_R \mathbb{Z}_p$ to randomize the signature as $(\sigma_1', \sigma_2') = (\sigma_1^t, \sigma_2^t)$. Then, the prover needs to prove the following:

$$\mathbf{PK}\{(m, \sigma) : \sigma \text{ is a PS-signature on m}\}. \tag{3}$$

In specific, the prover chooses $k \in_R \mathbb{Z}_p$ and computes $R = e(\sigma_1', \tilde{Y})^k$. The prover then obtains a random challenge $c \in \mathbb{Z}_p$ using the Fiat–Shamir heuristic and computes $s = k + c \cdot m$. Given $(\sigma_1', \sigma_2', c, s)$, a verifier can compute $R' = (e(\sigma_1'^{-1}, \tilde{X})e(\sigma_2', \tilde{g}))^{-c} e(\sigma_1'^s, \tilde{Y})$ and checks if the random challenge c is correctly computed.

C. Bulletproof System

Bulletproof [18] is an efficient zero-knowledge proof system for range proof on committed values with compact proof size. An instance of bulletproof can be written as follows:

$$\mathbf{PK}\{(a, r) : Y = h^r g^a \wedge a \in [0, 2^n]\} \tag{4}$$

where $Y = h^r g^a$ is a Pedersen commitment of integer $a \in \mathbb{Z}_p$ using randomness r. The above proof will convince the verifier that the secret in commitment Y lies in the range $[0, 2^n]$. Bulletproof system can be instantiated in the discrete-logarithm setting and made non-interactive with the Fiat–Shamir heuristic. We refer the readers to [18] for the detailed construction.

D. Ouroboros—A PoS Blockchain

Blockchain is a public ledger maintained by a peer-to-peer network that provides immutable and transparent list of transaction records. It contains an increasing list of blocks of transactions shared by network peers. Network peers rely on consensus protocols to reach consistency on the shared public ledger. In this paper, a state-of-the-art PoS based blockchain *Ouroboros* [19] is adopted because of its efficiency and rigorous security guarantees. In the following, we summarize the concepts and design principles of *Ouroboros* [19].

1) *Stakeholder.* A stakeholder is the miner in *Ouroboros*. Each stakeholder is assigned with a certain amount of stake, and the amount of the stake can change overtime.
2) *Epoch/Slot.* An epoch is a set of equal time slots. The *Ouroboros* assumes that the global clock is divided into discrete epochs and that all the stakeholders maintain a roughly synchronized clock.
3) *Users.* Users are the participants of the blockchain network. Users can make transactions to transfer crypto currencies and change the state of the public ledger.
4) *Block/Ledger.* A block is a collection of transactions. A sequence of blocks constitutes a leger.

In *Ouroboros*, a stakeholder is elected the slot leader for each time slot. The role of the slot leader is to collect transactions and issue only one block for the time slot. The core of the *Ouroboros* is a leader selection function that elects the slot leader proportionally to stakeholder's stake. That is, the more stake a stakeholder has, the more likely she will be elected as a slot leader.

V. Anonymous Reputation System

In this section, we propose an anonymous reputation system based on the PS-signature [16], Bulletproof system [18], and non-interactive zero-knowledge proof technique. We assume that secure and authenticated channels are established among entities.

A. System Setup

The IDM sets the security parameter λ of the system and generates the public parameters for consumers and retailers. Let $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T)$ be three cyclic groups with a prime order p, where p is λ bits. Furthermore, g_1 and g_2 are the generators of $\mathbb{G}_1$, and $\tilde{g}$ is a generator of $\mathbb{G}_2$. Also, $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ is a Type III bilinear pairing [16]. The IDM also chooses a collision-resistant hash function $\mathcal{H} : \{0,1\}^* \to \mathbb{Z}_p$. The IDM chooses a master secret key pair $\mathcal{S} = (x, y) \in_R \mathbb{Z}_p^2$ and computes $\tilde{X} = \tilde{g}^x$, $\tilde{Y} = \tilde{g}^y$. In summary, the system public parameters are as follows:

$$\mathcal{P} = \{\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, p, g_1, g_2, \tilde{g}, \tilde{X}, \tilde{Y}, \mathcal{H}, e\}. \tag{5}$$

B. Consumer Registration

A consumer C_i first registers herself at the IDM using her true identity. After that, C_i interacts with the IDM to obtain an anonymous identity credential as follows.

1) C_i chooses a secret $cs_i \in_R \mathbb{Z}_p$ and computes $(T_{i,1}, T_{i,2}) = (g_1^{cs_i}, \tilde{Y}^{cs_i})$. Then, C_i generates π_{cs_i}, a zero-knowledge proof of cs_i as follows:

$$\mathbf{PK}\{(cs_i) : T_{i,1} = g_1^{cs_i} \wedge T_{i,2} = \tilde{Y}^{cs_i}\}. \tag{6}$$

Afterward, C_i sends $(T_{i,1}, T_{i,2}, \pi_{cs_i})$ to the IDM.

2) The IDM first checks the validity of π_{cs_i} and $e(T_{i,1}, \tilde{Y}) \stackrel{?}{=} e(g_1, T_{i,2})$. If either of the equations does not hold, the IDM aborts. Otherwise, the IDM chooses $u \in_R \mathbb{Z}_p$ and computes a PS-signature on the committed message $T_{i,1}$ for consumer C_i as follows:

$$\begin{aligned}\sigma_i &= \text{SigCom}(T_{i,1}, \mathcal{P}, \mathcal{S}, u) \\ &= (\sigma_{i,1}, \sigma_{i,2}) = (g_1^u, (g_1^x \cdot T_{i,1}^y)^u).\end{aligned} \tag{7}$$

The IDM stores $(C_i, T_{i,1}, T_{i,2}, \sigma_i)$ and sends σ_i to C_i.

Authorized licensed use limited to: University of Waterloo. Downloaded on July 26,2020 at 19:15:18 UTC from IEEE Xplore. Restrictions apply.

3) Upon receiving σ_i from the IDM, C_i checks $\sigma_{i,1} \neq 1_{\mathbb{G}_1}$ and

$$e(\sigma_{i,1}, \tilde{X}\tilde{Y}^{cs_i}) \stackrel{?}{=} e(\sigma_{i,2}, \tilde{g}). \tag{8}$$

If the equation holds, C_i stores (cs_i, σ_i) as her anonymous identity credential.

C. Retailer Registration

Retailers register themselves at the IDM as follows.

1) A retailer R_j chooses $\tilde{g}_j \in_R \mathbb{G}_2$, $x_j, y_j, sk_j \in_R \mathbb{Z}_p^3$ and computes $\tilde{X}_j = \tilde{g}_j^{x_j}$, $\tilde{Y}_j = \tilde{g}_j^{y_j}, pk_j = g_2^{sk_j}$. The secret parameter of R_j is $\mathcal{S}_j = (x_j, y_j, sk_j)$, and the public parameter is $\mathcal{P}_j = (\tilde{g}_j, \tilde{X}_j, \tilde{Y}_j, pk_j)$.
2) Then, R_j generates a proof π_{R_j} as follows:

$$\mathbf{PK}\{(x_j, y_j, sk_j) : \tilde{X}_j = \tilde{g}_j^{x_j} \wedge \tilde{Y}_j = \tilde{g}_j^{y_j} \wedge pk_j = g_2^{sk_j}\}. \tag{9}$$

R_j sends its public key P_j and π_{R_j} to the IDM.
3) The IDM checks the validity of proof π_{R_j}. The IDM aborts when the proof is invalid. Otherwise, the IDM stores $(R_j, \mathcal{P}_j)$.

D. Rating Token Generation

Consumers can make purchases from retailers via anonymous payment channels, such as zerocash [29]. After making a purchase from R_j, C_i can obtain an anonymous rating token as follows.

1) C_i chooses $g_{i,j} \in_R \mathbb{G}_1$ and $t \in_R \mathbb{Z}_p$ to compute $(\sigma'_{i,1}, \sigma'_{i,2}) = (\sigma_{i,1}^t, \sigma_{i,2}^t)$, $Y = g_{i,j}^{-cs_i}$ using σ_i. Then, C_i constructs a proof as follows:

$$\mathbf{PK}\left\{\begin{array}{l}(cs_i, \sigma_i) : \\ \sigma_i \text{ is a PS-signature on cs}_i \wedge \\ Y = g_{i,j}^{-cs_i}\end{array}\right\}. \tag{10}$$

2) In specific, C_i chooses $k \in_R \mathbb{Z}_p$ and computes the following:

$$\begin{aligned} R &= e(\sigma'_{i,1}, \tilde{Y})^k = e(\sigma_{i,1}, \tilde{Y})^{kt} \\ T &= g_{i,j}^k \\ c &= \mathcal{H}(\sigma'_{i,1}, \sigma'_{i,2}, R, Y, T, g_{i,j}) \\ s &= k + c \cdot cs_i. \end{aligned} \tag{11}$$

The proof is the combination of the general pre-image zero-knowledge technique with the proof-of-knowledge of signature technique by re-using response s. C_i sends $(\sigma'_{i,1}, \sigma'_{i,2}, Y, g_{i,j}, c, s)$ to R_j.
3) R_j computes R', T' and checks the following:

$$\begin{aligned} R' &= (e(\sigma'^{-1}_{i,1}, \tilde{X})e(\sigma'_{i,2}, \tilde{g}))^{-c} e(\sigma'^{s}_{i,1}, \tilde{Y}) \\ T' &= Y^c g_{i,j}^s \\ c &\stackrel{?}{=} \mathcal{H}(\sigma'_{i,1}, \sigma'_{i,2}, R', Y, T', g_{i,j}). \end{aligned} \tag{12}$$

If the equation holds, R_j will generate an anonymous rating token $\sigma_{i,j}$ for C_i using x_j, y_j as follows:

$$\begin{aligned} \sigma_{i,j} &= \mathbf{SigCom}(Y, \mathcal{P}_j, \mathcal{S}_j, u') \\ &= (\sigma_{i,j,1}, \sigma_{i,j,2}) = (g_{i,j}^{u'}, (g_{i,j}^{x_j} \cdot Y^{-y_j})^{u'}) \end{aligned} \tag{13}$$

where $u' \in_R \mathbb{Z}_p$. Then, R_j sends the anonymous rating token $\sigma_{i,j}$ to C_i via a secure channel.
4) Upon receiving $\sigma_{i,j}$, C_i checks $\sigma_{i,j,1} \neq 1_{\mathbb{G}_1}$ and

$$e(\sigma_{i,j,1}, \tilde{X}_j \tilde{Y}_j^{cs_i}) \stackrel{?}{=} e(\sigma_{i,j,2}, \tilde{g}_j). \tag{14}$$

If the equation holds, C_i stores $\sigma_{i,j}$ as her rating token for retailer R_j.

E. Anonymous Review Generation and Verification

The IDM chooses a set of retailers to form a committee $\mathcal{L}_C$. A consumer C_i can leave a rating score for retailer R_j using the rating token $\sigma_{i,j}$ and identity credential σ_i as follows.

1) C_i chooses a rating score $s_{i,j}$, where $s_{i,j} \in \mathbb{Z}_p$ can be an integer in the range $[1, 10]$. C_i obtains the public keys, pk_j, of all the committee members and computes $pk_C = \prod_{R_j \in \mathcal{L}_C} pk_j$. Then, C_i chooses $r \in_R \mathbb{Z}_p$ and encrypts $s_{i,j}$ as follows:

$$r_{i,j} = (r_{i,j,1}, r_{i,j,2}) = (pk_C^r g_2^{s_{i,j}}, g_2^r). \tag{15}$$

C_i constructs a proof $\pi_{i,j}$ to prove that $r_{i,j}$ is a valid encryption of $s_{i,j}$ that lies in the range $[1, 10]$. We have the following:

$$\mathbf{PK}\left\{\begin{array}{l}(s_{i,j}, r) : r_{i,j,1} = pk_C^r g_2^{s_{i,j}} \wedge \\ r_{i,j,2} = g_2^r \wedge s_{i,j} \in [1, 10]\end{array}\right\}. \tag{16}$$

The above proof can be instantiated via sigma protocol and bulletproof system.
2) C_i chooses random numbers $r_1, r_2 \in \mathbb{Z}_p$ and computes the following:

$$\begin{aligned} &\beta_1 = \sigma_{i,1}^{r_1}, \beta_2 = \sigma_{i,2}^{r_1}, \beta_3 = \sigma_{i,j,1}^{r_2} \\ &\beta_4 = \sigma_{i,j,2}^{r_2}, \beta_5 = g_1^{\mathcal{H}(R_j)cs_i}. \end{aligned} \tag{17}$$

C_i needs to prove the knowledge of a valid rating token and an identity credential by constructing the proof as follows:

$$\mathbf{PK}\left\{\begin{array}{l}(cs_i, \sigma_i, \sigma_{i,j}) : \\ \sigma_i, \sigma_{i,j} \text{ are } PS - \text{signatures on cs}_i \wedge \\ \beta_5 = g_1^{\mathcal{H}(R_j)cs_i}\end{array}\right\}. \tag{18}$$

3) In specific, C_i chooses a random number $k_{ep} \in \mathbb{Z}_p$ and computes the following:

$$\begin{aligned} &\alpha_1 = e(\beta_1, \tilde{Y})^{k_{ep}}, \alpha_2 = e(\beta_3, \tilde{Y}_j)^{k_{ep}} \\ &\alpha_3 = g_1^{\mathcal{H}(R_j)k_{ep}} \\ &ch = \mathcal{H}(\beta_1, \beta_2, \beta_3, \beta_4, \beta_5, \alpha_1, \alpha_2, \alpha_3, R_j, r_{i,j}, \pi_{i,j}) \\ &s_i = k_{ep} + ch \cdot cs_i. \end{aligned} \tag{19}$$

Authorized licensed use limited to: University of Waterloo. Downloaded on July 26,2020 at 19:15:18 UTC from IEEE Xplore. Restrictions apply.

C_i sets $\sigma = (\beta_1, \beta_2, \beta_3, \beta_4, \beta_5, ch, s_i)$ and sends the anonymous review $(\sigma, r_{i,j}, \pi_{i,j}, R_j)$ to the committee members.

4) Upon receiving the ratings from C_i, the committee members check the validity of the anonymous review. The committee members first compute the following equations using system public parameters $\mathcal{P}$ and retailer R_j's public key $\mathcal{P}_j$:

$$\alpha_1' = e(\beta_1, \tilde{X})^{ch} e(\beta_2, \tilde{g})^{-ch} e(\beta_1, \tilde{Y})^{s_i}$$
$$\alpha_2' = e(\beta_3, \tilde{X}_j)^{ch} e(\beta_4, \tilde{g}_j)^{-ch} e(\beta_3, \tilde{Y}_j)^{s_i}$$
$$\alpha_3' = \beta_5^{-ch} \cdot g_1^{\mathcal{H}(R_j)s_i}. \quad (20)$$

The committee members check the validity of proof $\pi_{i,j}$ as specified in [18] and whether $ch \stackrel{?}{=} \mathcal{H}(\beta_1, \beta_2, \beta_3, \beta_4, \beta_5, \alpha_1', \alpha_2', \alpha_3', R_j, r_{i,j}, \pi_{i,j})$. If both of the conditions hold, the committee members accept the anonymous review.

F. Review Aggregation

Committee members aggregate the valid encrypted rating scores for each retailer. For retailer R_j, committee members compute $s_j = (s_{j,1}, s_{j,2}) = (\prod r_{i,j,1}, \prod r_{i,j,2})$ for all the valid encrypted rating scores $r_{i,j}$. For retailer R_j, a committee member C_m computes a partial decryption token $p_{j,m} = s_{j,2}^{sk_m}$, where sk_m is the secret key of C_m. The committee member constructs a proof $\pi_{j,m}$ that the partial decryption token is correctly constructed as follows:

$$\mathbf{PK}\{(sk_m) : p_{j,m} = s_{j,2}^{sk_m} \wedge pk_m = g_2^{sk_m}\}. \quad (21)$$

The final decryption $\mathcal{RS}_j$ of the aggregated rating score for retailer R_j should be as follows:

$$\mathcal{RS}_j = \frac{s_{j,1}}{\prod_{C_m \in \mathcal{L}_C} p_{j,m}} = g_2^{\sum s_{i,j}}. \quad (22)$$

It should be noted that the final aggregated rating score $\sum s_{i,j}$ is at the exponent of g_2. All retailers and consumers can efficiently pre-compute a table that contains g_2^l, where l can range from 0 to a few thousands.

G. Linking and Tracing

For all the valid reviews, committee members will check if there exists the same β_5. If the committee members find the same β_5 from different reviews, it indicates that a consumer submitted multiple reviews for the same purchase. The committee members will report the anonymous review of the misbehaving consumer to the IDM. To recover the true identity of the misbehaving consumer, the IDM checks the following equation for each $(T_{i,1}, T_{i,2})$ stored in its storage:

$$e(\beta_2, \tilde{g}) \cdot e(\beta_1, \tilde{X})^{-1} \stackrel{?}{=} e(\beta_1, T_{i,2}). \quad (23)$$

The IDM publishes $T_{i,1}$ and $T_{i,2}$ that matches the above equation as a misbehaving consumer.

In this section, we propose a reputation system that enables consumers privately make purchases and leave reviews. In the next section, we will present the details on implementing the proposed system on a PoS blockchain to improve system transparency and reliability.

VI. Anonymous Reputation System Atop PoS Blockchain

In this section, we integrate our anonymous reputation system atop a PoS blockchain—*Ouroboros* [19]. The operations proposed in Section V are classified into two categories: 1) on-chain and 2) off-chain operations. The off-chain operations include consumer/retailer registration and rating token generation that requires interactions between the IDM, retailers, and consumers via secure channels.

Review generation, verification, and aggregation are on-chain operations that happen over a public ledger $\mathcal{L}$. We adopt a hybrid blockchain model in the ARS-PS. Retailers act as stakeholders based on the PoS protocol in *Ouroboros* with their reputations associated with the stake. Retailers need to obtain permissions from the IDM before they can serve as stakeholders. Consumers act as blockchain users who can freely join the blockchain network. Consumers can leave reviews and enumerate accumulated retailers' reputation scores by making different types of transactions to the ledger. The reasons that we adopt *Ouroboros* are threefold as follows.

1) A PoS blockchain is more suitable for constructing a consortium network.
2) A PoS blockchain offers qualitative efficiency and scalability compared with that of a proof of work blockchain.
3) Committee member management in the ARS-PS can be realized via the consensus protocol in [19].

The blockchain-based anonymous reputation system consists of the following steps. Notations from Section VI are re-used.

A. Genesis Block Generation

The IDM runs the *System Setup* of Section VI, generates and publishes the system parameters $\mathcal{P}$. Consumers and retailers can obtain $\mathcal{P}$ via secure channels, such as transport layer security. The IDM also defines $T_{\mathcal{A}}$ as the size of the anonymity set, which indicates the privacy level of the system. Retailers interact with the IDM to register their public keys $\mathcal{P}_j$. The IDM creates a global reputation board $\mathcal{B}$ that contains the global reputation scores $\mathcal{RS}_j$ for each retailer. Consumers register themselves at the IDM to obtain anonymous identity credentials σ_i. Both retailers and consumers can join the blockchain network to obtain their blockchain accounts with a public/private key pair to sign on the transactions. Retailer blockchain account information is publicly associated with their identities, while consumer blockchain accounts remain anonymous.

The IDM sets the global clock of the system and divides the clock into epochs of equal time slots. Each epoch is divided into three stages: *1) Accumulation*, *2) Aggregation,* and *3) Revelation*. The number of time slots for each stage is $\mathcal{K}_1, \mathcal{K}_2$, and $\mathcal{K}_3$, respectively. At the beginning of each epoch, the IDM runs a committee selection function [19] to select a committee of retailers with high reputation scores, which is responsible for the slot leader selection and review revelation process. Afterward,

Authorized licensed use limited to: University of Waterloo. Downloaded on July 26,2020 at 19:15:18 UTC from IEEE Xplore. Restrictions apply.

the IDM generates a genesis block of ledger $\mathcal{L}$ consisting of system parameters $\mathcal{P}$, retailer parameters $\mathcal{P}_j$, retailers blockchain account information, and the list of committee members $\mathcal{L}_C$ in this epoch. Committee members run a leader selection function [19] to select slot leaders for time slots in this epoch.

B. Review Accumulation

For each registered retailer R_j, the IDM creates a review smart contract SC_j. The smart contract SC_j records the reviews for retailer R_j. In particular, the contract SC_j has two functions $Update$ and $GetReview$. The $Update$ function takes into the anonymous review transactions from consumers. The anonymous reviews can later be accessed by the $GetReview$ function. Consumer C_i can make purchases from retailer R_j in an off-chain manner and obtain a valid rating token $\sigma_{i,j}$. The consumer can obtain an one-time blockchain address and public/private key pairs. In this stage, C_i can generate an anonymous review transaction T_r including the anonymous review $(\sigma, r_{i,j}, \pi_{i,j}, R_j)$ to the smart contract SC_j by calling the $Update$ function. The smart contract SC_j records the anonymous review in its storage for future reputation aggregation and revelation.

C. Review Aggregation

In the *Aggregation* stage, each slot leader is responsible for the review aggregation task of $1/\mathcal{K}_2$ of overall retailers. Slot leaders aggregate the encrypted reviews for each retailer in the following steps.

1) A slot leader queries the current state of contracts, SC_j, in her management scope. The slot leader will report double-reviews for the same retailer to the IDM to recover the true identity of the misbehaving consumer.
2) For retailer R_j, the slot leader checks the number of valid received reviews. If the number exceeds $T_{\mathcal{A}}$, the slot leader aggregates the valid encrypted rating scores to obtain an aggregated rating score s_j.
3) The slot leader constructs a reveal smart contract $\mathcal{R}$. The contract $\mathcal{R}$ includes the aggregated rating scores for retailers in her management scope with a counter C_{R_j} that records the number of reviews received for the retailer. The reveal contract also provides a function *UpdateToken* to receive partial decryption tokens from committee members.

After all the slot leaders in this stage publish the $\mathcal{R}$ contracts, the system proceeds to the final *Revelation* stage.

D. Review Revelation

In the *Revelation* stage, committee members first check the reveal contracts, $\mathcal{R}$, generated from the previous stage. For the aggregated rating scores, committee members update their partial decryption tokens to the reveal contracts using the *UpdateToken* function. After obtaining all the partial decryption tokens for the reveal contracts, the IDM verifies the correctness of the partial decryption tokens and decrypts the aggregated scores using (22). Finally, the IDM updates the reputation scores in the global reputation board for retailers.

E. Epoch Update

For the next epoch, retailers interact with the IDM to generate a new set of retailer public keys, $\mathcal{P}_j$, for each retailer R_j. The IDM runs the committee selection function for the new epoch. New committee members, then, run the leader selection function for this epoch according to the updated global reputation scores. For the encrypted reviews that are not aggregated in the previous epoch, consumers generate new review transactions with the updated committee encryption parameters.

VII. Security Analysis

In this section, we give the security analysis of the proposed ARS-PS based on the design goals.

A. Bounded Confidentiality

Consumers encrypt their rating scores with committee members' public keys. Committee members will check the validity of the reveal contracts and only publish their partial decryption tokens for the valid aggregated rating scores. That is, an adversary can obtain the individual review statistics only if he can solve the **DDH** problem in $\mathbb{G}_1$ [30], or if he can control the whole committee members to recover the decryption key. At the same time, consumers need to prove that the encrypted rating scores lie in a correct range. Because of the *Soundness* and *Completeness* property of Bulletproof [18], the verifier will accept the range proof if it is correctly constructed. That is, the bounded confidentiality is preserved in our system.

B. Conditional Anonymity

The consumer C_i first registers herself at the IDM to obtain an anonymous identity credential σ_i. To obtain an anonymous rating token, consumer C_i chooses a random generator $g_{i,j}$ for each purchase and proves to the retailer that the committed message $Y = g_{i,j}^{-cs_i}$ contains the same consumer secret with the identity token in a zero-knowledge manner. Then, retailers can sign on the committed message $Y = g_{i,j}^{-cs_i}$. When leaving an anonymous review, C_i needs to prove the knowledge of a valid rating token and an anonymous identity credential using the sigma protocol [17]. Thus, the anonymity of obtaining a rating token and leaving a review can be reduced to the *zero-knowledge* property of the underlying sigma protocol in the discrete-logarithm setting. When a consumer misbehavior is detected, slot leaders report the anonymous reviews to the IDM to recover the identity of the consumer. Retailers cannot recover the identity of a consumer since consumers do not generate $\tilde{Y}_j^{cs_i}$ when obtaining the rating token. That is, conditional anonymity is preserved in the ARS-PS.

C. Unforgeability

To generate the anonymous identity credential, the IDM needs to sign on the committed message $g_1^{cs_i}$ using the PS-signature. Similarly, the retailer needs to sign on the committed message

Authorized licensed use limited to: University of Waterloo. Downloaded on July 26,2020 at 19:15:18 UTC from IEEE Xplore. Restrictions apply.

$g_{i,j}^{cs_i}$ to generate a rating token for consumer C_i. That is, the unforgeability of the identity credential and rating token can be reduced to the unforgeability of the PS-signature [16], which can be further reduced to *q-MSDH-1* assumption in the non-interactive setting [16]. To generate the anonymous review σ and $\pi_{i,j}$, the consumer needs to prove the knowledge of an identity credential and a rating token at the same time. Thus, the consumer cannot forge the anonymous review if the underlying sigma protocol [17] is sound.

D. Confined Unlinkability

Unlinkability requires that retailers and consumers cannot determine whether two reviews are from the same consumer. This property comes from two folds. First, a consumer can choose different random generators to require a rating token. Second, the consumer can further randomize the rating token by choosing a random number r_2 when generating an anonymous review and prove the knowledge of consumer secret in a zero-knowledge manner. That is, unlinkability can be reduced to the security of underlying sigma protocol. When generating a review, C_i needs to construct β_5 and prove to the public that β_5 contains the same secret cs_i with $\beta_1, \beta_2, \beta_3$, and β_4. If C_i leaves multiple reviews for the same retailer, β_5 in the anonymous review is publicly identical. The combination of conditional anonymity and confined unlinkability helps the system mitigate Sybil attacks.

E. Transparency

The review accumulation, aggregation, and revelation are implemented by the review and reveal contracts on the public ledger. Consumers can make review transactions to change or query the state of the contracts. Since the transactions and ledger state changes are open to the public's view, transparency of reputation system is guaranteed [31].

F. Blockchain Security

As a public transaction ledger, the blockchain security is formally defined as *Persistence* and *Liveness* [19]. Specifically, we borrow the definitions from [19]. *Persistence* preserves the stability of the public ledger. *Liveness* means that a valid transaction is guaranteed to be included in the ledger after a certain time. If the adversary cannot control most of the stakes in the system, *Ouroboros* is proven to achieve the above properties [19]. The ledger is maintained by registered retailers, and the retailer's reputation in our system is associated with the stake in the PoS consensus protocol of *Ouroboros*. A retailer with the higher reputation score is less likely to behave distrustfully since the cost for the misbehavior is expensive. As a result, the public transaction ledger is robust in the ARS-PS. We, then, discuss the security of the review and reveal contracts.

In the *Accumulation* stage, consumers make transactions to the review contracts. Based on the ledger robustness, the transactions will finally be confirmed after a certain number of slots with a high probability. Prorogation delays could happen such that some reviews may not be included on the ledger in this epoch. In this case, consumers can update their reviews in the next epoch.

In the *Aggregation* phase, slot leaders verify the correctness of the reviews and aggregate the encrypted rating scores. That is, the security in this stage (i.e., the correctness of the aggregated rating scores) depends highly on the trustworthiness of the slot leaders. If a slot leader does not fulfill his task (e.g., aggregate incorrect reviews or purposely exclude some reviews), his misbehavior may not be discovered immediately. However, since the historical reviews and aggregated rating scores are open to the public, anyone in the system can check the correctness in the future and make a complaint if the misbehavior of a slot leader is detected. By properly setting the punishment for misbehaving slot leaders, a rationale slot leader is motivated to correctly fulfill the task. Moreover, the blockchain accounts of the consumers remain anonymous in the ARS-PS. A malicious consumer may generate a large number of invalid reviews to use up the slot leader's computational capacities. To prevent this attack, the review contracts can require consumers to deposit currencies to the contract and only return the currencies to the consumer when the review is verified. Secure and anonymous payment channels (such as zerocash [29]) can be utilized to preserve consumer anonymity and unlinkability in this process.

In the *Revelation* stage, committee members verify the correctness of reveal contracts and update their partial decryption tokens to the reveal contract. The correctness of the tokens is ensured by the zero-knowledge proof $\pi_{j,m}$. The public cannot decrypt the aggregated rating scores unless all the committee members have successfully submitted their tokens to the ledger. Compared with communication overhead in the *Accumulation* stage, only finite transactions are required in this stage. To mitigate the impact of the communication delay among committee members, we can set a larger number of $\mathcal{K}_3$ to ensure the ledger robustness at this stage. For the committee member who fails to submit the token, the IDM can directly contact the committee member. We can also implement a threshold encryption scheme [32] to improve system robustness.

VIII. Performance Evaluation

In this section, we evaluate the performance of the proposed ARS-PS. We first compare the ARS-PS with existing schemes in terms of functionalities. Then, we present a proof-of-concept implementation based on Parity Ethereum and demonstrate the implementation's feasibility. Finally, we discuss the scalability of the ARS-PS.

A. Functionality

In Table I, we summarize the recent advances in reputation systems in terms of architectures and desired functionalities. Compared with a centralized architecture [7], a decentralized architecture [8], [10] is preferred for its advantage in eliminating a single trusted marketplace. Blockchain-based solutions [6], [12] and the ARS-PS further increase system transparency. As we discussed in the section that covers security analysis, versatile functionalities are achieved in the ARS-PS by integrating a PoS blockchain with a set of cryptographic primitives.

Authorized licensed use limited to: University of Waterloo. Downloaded on July 26,2020 at 19:15:18 UTC from IEEE Xplore. Restrictions apply.

TABLE I
OVERVIEW OF FUNCTIONALITIES

Proposal	Architecture	Conditional Anonymity	Bounded Confidentiality	Confined Unlinkability	Transparency
Blomer [6]	Centralized	√	√	√	
Zhai [9]	Decentralized	√	√	√	
Azad [7]	Decentralized		√		√
Schaub [11]	Blockchain	√		√	√
Soska [5]	Blockchain	√		√	√
ARS-PS	Blockchain	√	√	√	√

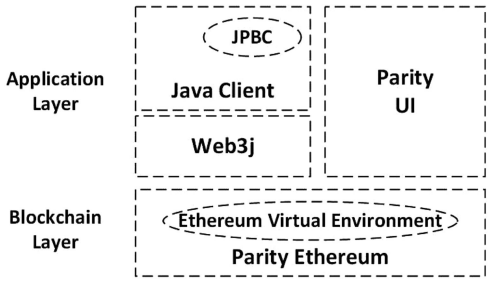


Fig. 2. Implementation overview.

B. Implementation Overview

We present a proof-of-concept implementation of the ARS-PS as shown in Fig. 2. We simulate the IDM, consumer, and retailer with JAVA clients on a laptop with 2.40-GHz Intel Core i5 processors and 8 GB memory. We implement an MNT curve with an embedding degree 6 based on Java pairing based cryptography (JPBC) [33]. We instantiate the Bulletproof system with a range of 3 bit and a linear-size argument.

We set up a testing Ethereum Proof of Authority (PoA) blockchain network [34]. In particular, the following two kinds of Parity nodes are implemented in Parity PoA network.

1) Authority nodes serve as retailers that can be selected as slot leaders to validate transactions and issue blocks.
2) User nodes serve as consumers that can make anonymous review transactions to the blockchain.

For illustrative purposes, a few authority nodes and user nodes are deployed in our experiments. Slot leaders are statically specified and written as configurations in the chain specification file. We increase the block gas limit in our testing network for storing the reviews. JAVA clients communicate with the associated Parity nodes via web3j [35] to send transactions and interact with smart contracts. Moreover, we encode the public parameters of the system and authority nodes into Java clients. A review smart contract written in Solidity [36] is deployed via Parity UI, which provides an $Update$ function and a $GetReview$ function.

We evaluate the system efficiency in terms of on-chain and off-chain performances. On-chain operations denote the review transaction generation/verification. Off-chain operations denote the registration and token generation phases.

C. Off-Chain Performance

We evaluate the off-chain performance including consumer/retailer registration, rating token generation among entities. In Table II, experimental results show that the computation incurs a few milliseconds.

TABLE II
OFF-CHAIN OVERHEAD

Operations	Involved Entities	Time (ms)
Consumer Registration	Consumer/IDM	487
Retailer Registration	Retailer/IDM	263
Rating Token Generation	Consumer/Retailer	259

TABLE III
REVIEW GENERATION/VERIFICATION

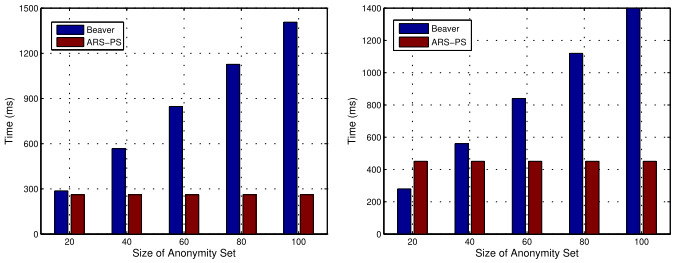
	Rating Score	Proof σ	Proof $\pi_{i,j}$
Generation (ms)	15	183	63
Verification (ms)	N/A	347	110
Size (Bytes)	104	306	565

D. On-Chain Performance

We simulate an epoch of the ARS-PS. In particular, the consumers with rating tokens and identity credentials leave anonymous reviews by calling the $Update$ function in the review contract. Then, the slot leader retrieves all the reviews from the review contract and verifies the correctness of the proofs. The slot leader creates another reveal contract $\mathcal{R}$ that aggregates the encrypted rating scores of valid reviews and receives partial decryption tokens from committee members.

We move the on-chain proof verifications to be conducted by the slot leader out of the EVM. In Table III, we show the computational cost of generating and verifying an anonymous review. We further compare the ARS-PS with state-of-the-art literature that is based on ring signature [6] for review generation/verification. A ring-signature based method [6] requires purchase transactions to be also deployed on the public ledger. Consumers collect a set of public keys of previous purchase transactions (anonymity set $T_{\mathcal{A}}$) to generate/verify the anonymous reviews, which results in linearly increasing computational cost as shown in Fig. 3(a) and (b). The review generation/verification may consume a few hundred milliseconds in the ARS-PS. The reasons are twofold: (1) The proof σ consists of an identity proof and rating token proof to achieve conditional anonymity, which results in a double proof of knowledge of PS-signature; and (2) paring operations over an MNT curve are expensive in the implemented JPBC library without PBC wrapper.

Authorized licensed use limited to: University of Waterloo. Downloaded on July 26,2020 at 19:15:18 UTC from IEEE Xplore. Restrictions apply.



(a) Review Generation (b) Review Verification

Fig. 3. Review Computation Cost. (a) Review Generation. (b) Review Verification.

E. Scalability Discussions

In the following, we discuss the system scalability for different stages in one epoch. We define N_C as the number of committee members for the epoch.

1) Accumulation Stage: In our testing PoA blockchain with optimal network conditions, a consumer that calls the $Update$ function will have her review transaction included in the ledger within a few blocks. In real-world implementations [19], the communication delays between consumers and slot leaders may lead to the exclusion of a certain transaction in the epoch. To mitigate this issue, we can increase the number of slots $\mathcal{K}_1$ in this stage and the number of peer connections for the consumer Parity node.

2) Aggregation Stage: Slot leaders in this stage verify and aggregate the anonymous reviews. The performance is mainly affected by two factors: the number of time slots $\mathcal{K}_2$ and the size of the anonymity set $\mathcal{T}_A$. A larger $\mathcal{K}_2$ reduces the individual computation overhead for slot leaders while increasing the overall epoch time. The quantity of $\mathcal{T}_A$ indicates privacy guarantees for consumers. However, a larger $\mathcal{T}_A$ could also increase the probability that insufficient number of reviews are received for aggregation in this epoch, which requires consumers to regenerate the reviews in the next epoch.

3) Revelation Stage: Committee members upload their partial decryption tokens to the reveal contract. The total number of transactions in this stage is $N_C * \mathcal{K}_2$. IDM can choose different N_C for the trade-off between system security strength and efficiency. To further improve the reveal efficiency and prevent decryption failure in case that a committee member does not update her decryption token, a threshold ElGamal encryption system can be adopted [32]. We can also partition the committee into different subgroups. Each subgroup is responsible for the decryption key management of a set of retailers to reduce the communication overhead.

IX. Conclusion

In this paper, we have investigated the privacy and transparency issues in current reputation systems for the IIoT-enabled retail marketing. We have developed an anonymous reputation system that provides a high privacy guarantees for consumers, which can also be efficiently and securely integrated with a PoS blockchain. We have implemented a proof-of-concept prototype system based on Ethereum and the experimental results have demonstrated the feasibility of our proposed system compared with state-of-the-art literature. For the future work, we will design a committee partition strategy with fine-grained review aggregation management to further improve the overall system efficiency.

References

[1] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in industrial internet of things," *IEEE Trans. Ind. Inform.*, vol. 14, no. 8, pp. 3690–3700, Aug. 2018.

[2] J. Gregory, "The Internet of Things: revolutionizing the retail industry," *Accenture Strategy*, 2015.

[3] L. Ardito, A. M. Petruzzelli, U. Panniello, and A. C. Garavelli, "Towards industry 4.0: Mapping digital technologies for supply chain management-marketing integration," *Bus. Process Manage. J.*, 2018.

[4] K. Korpela, J. Hallikas, and T. Dahlberg, "Digital supply chain transformation toward blockchain integration," in *Proc. 50th Hawaii Int. Conf. Syst. Sci.*, 2017, pp. 4182–4191.

[5] B. Nguyen and L. Simkin, "The internet of things (IoT) and marketing: The state of play, future trends and the implications for marketing," *J. Marketing Manage.*, vol. 33, pp. 1–6, 2017.

[6] K. Soska, A. Kwon, N. Christin, and S. Devadas, "Beaver: A decentralized anonymous marketplace with secure reputation," *IACR Cryptol. ePrint Arch.*, 2016, Art. no. 464.

[7] J. Blömer, F. Eidens, and J. Juhnke, "Practical, anonymous, and publicly linkable universally-composable reputation systems," in *Proc. Cryptographers' Track RSA Conf.*, 2018, pp. 470–490.

[8] M. A. Azad, S. Bag, and F. Hao, "PrivBox: Verifiable decentralized reputation system for the on-line marketplaces," *Future Gener. Comput. Syst.*, vol. 89, pp. 44–57, 2018.

[9] T. Minkus and K. W. Ross, "I know what youre buying: Privacy breaches on ebay," in *Proc. Int. Symp. Privacy Enhancing Technol. Symp.*, 2014, pp. 164–183.

[10] E. Zhai, D. I. Wolinsky, R. Chen, E. Syta, C. Teng, and B. Ford, "AnonRep: Towards tracking-resistant anonymous reputation," in *Proc. Netw. Syst. Des. I mplementation*, 2016, pp. 583–596.

[11] J. Blömer, J. Juhnke, and C. Kolb, "Anonymous and publicly linkable reputation systems," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, 2015, pp. 478–488.

[12] A. Schaub, R. Bazin, O. Hasan, and L. Brunie, "A trustless privacy-preserving reputation system," in *Proc. IFIP Int. Inf. Secur. Privacy Conf.*, 2016, pp. 398–411.

[13] R. Bazin, A. Schaub, O. Hasan, and L. Brunie, "A decentralized anonymity-preserving reputation system with constant-time score retrieval," *IACR Cryptol. ePrint Arch.*, 2016, Art. no. 416.

[14] K. Zhang, X. Liang, R. Lu, K. Yang, and X. Shen, "Exploiting mobile social behaviors for sybil detection," in *Proc. IEEE INFOCOM*, 2015, pp. 271–279.

[15] J. Mendling *et al.*, "Blockchains for business process management-challenges and opportunities," *ACM Trans. Manage. Inf. Syst.*, vol. 9, no. 1, 2018, Art. no. 4.

[16] D. Pointcheval and O. Sanders, "Reassessing security of randomizable signatures," in *Proc. Cryptograph. Track RSA Conf.*, 2018, pp. 319–338.

[17] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in *Proc. Conf. Theory Appl. Cryptogr. Techn.*, 1986, pp. 186–194.

[18] B. Bünz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, and G. Maxwell, "Bulletproofs: Short proofs for confidential transactions and more," in *Proc. IEEE Symp. Secur. Privacy*, 2018, pp. 319–338.

[19] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A provably secure proof-of-stake blockchain protocol," in *Proc. Annu. Int. Cryptol. Conf.*, 2017, pp. 357–388.

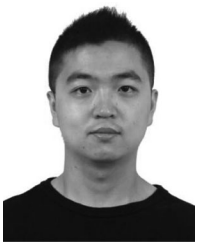
[20] Parity. [Online]. Avaailable: https://github.com/paritytech/parity-ethereum, Accessed August 2018.

[21] R. Dennis and G. H. Owenson, "Rep on the block: A next generation reputation system based on the blockchain," in *Proc. 10th Int. Conf. Internet Technol. Secured Trans.*, 2015, pp. 131–138.

[22] R. Di Pietro, X. Salleras, M. Signorini, and E. Waisbard, "A blockchain-based trust system for the internet of things," in *Proc. 23rd ACM Symp. Access Control Models Technol.*, 2018, pp. 77–83.

Authorized licensed use limited to: University of Waterloo. Downloaded on July 26,2020 at 19:15:18 UTC from IEEE Xplore. Restrictions apply.

[23] S. Bag, M. A. Azad, and F. Hao, "A privacy-aware decentralized and personalized reputation system," *Comput. Secur.*, vol. 77, pp. 514–530, 2018.
[24] M. P. Andersen, J. Kolb, K. Chen, G. Fierro, D. E. Culler, and R. A. Popa, "Wave: A decentralized authorization system for IoT via blockchain smart contracts," Dept. Elect. Eng. Comput. Sci., Univ. California, Oakland, CA, USA, Tech. Rep. UCB/EECS-2017-234, 2017.
[25] B. David, P. Gaži, A. Kiayias, and A. Russell, "Ouroboros praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain," in *Proc. Annu. Int. Conf. Theory Appl. Cryptogr. Techn.*, 2018, pp. 66–98.
[26] J. Camenisch, A. Kiayias, and M. Yung, "On the portability of generalized schnorr proofs," in *Proc. Annu. Int. Conf. Theory Appl. Cryptogr. Techn.*, 2009, pp. 425–442.
[27] J. Ni, X. Lin, and X. S. Shen, "Efficient and secure service-oriented authentication supporting network slicing for 5g-enabled IoT," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 3, pp. 644–657, Mar. 2018.
[28] D. Pointcheval and O. Sanders, "Short randomizable signatures," in *Proc. Cryptographers' Track RSA Conf.*, 2016, pp. 111–126.
[29] E. B. Sasson *et al.*"Zerocash: Decentralized anonymous payments from bitcoin," in *Proc. IEEE Symp. Secur. Privacy*, 2014, pp. 459–474.
[30] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inf. Theory*, vol. IT-31, no. 4, pp. 469–472, Jul. 1985.
[31] Y. Lu, Q. Tang, and G. Wang, "Zebralancer: Private and anonymous crowdsourcing system atop open blockchain," in *Proc. IEEE ICDCS*, 2018, pp. 853–865.
[32] T. P. Pedersen, "A threshold cryptosystem without a trusted party," in *Proc. Workshop Theory Appl. Cryptogr. Techn.*, 1991, pp. 522–526.
[33] Java pairing based cryptograph. [Online]. Available: https://github.com/emilianobonassi/jpbc, Accessed August 2018.
[34] Proof-of-Authority (PoA) chains. [Online]. Available: https://wiki.parity.io/Proof-of-Authority-Chains, Accessed Aug. 2018.
[35] Web3j—lightweight java library for integration with Ethereum clients. [Online]. Available: https://docs.web3j.io/, Accessed Aug. 2018.
[36] Solidity. [Online]. Available: https://solidity.readthedocs.io/en/v0.4.25/, Accessed Aug. 2018.

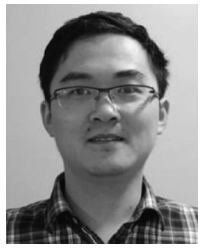


Dongxiao Liu (S'13) received the B.S. and M.S. degrees in computer science from the School of Computer Science and Engineering, University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 2013 and 2016, respectively. He is currently working toward the Ph.D. degree at the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada.

His research interests include applied cryptography and privacy enhancing technologies for blockchain.

Amal Alahmadi received the B.E. degree in information technology and computing from Arab Open University, Jeddah, Saudi Arabia, in 2010. She is currently working toward the M.S. degree in applied computing (MAC) at Wilfrid Laurier University, Waterloo, ON, Canada.

During 2006–2015, she held various positions in the technology sector until the last post was as IT Systems Executive in Emaar Company, Dubai. Her research interests include cybersecurity for the blockchain and Internet of Things.



Jianbing Ni (M'18) received the B.E. and M.S. degrees in computer science from the University of Electronic Science and Technology of China, Chengdu, China, in 2011 and 2014, respectively, and the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2018.

He is currently a Postdoctoral Research Fellow with the Department of Electrical and Computer Engineering, University of Waterloo. His research interests are applied cryptography and network security, with current focus on cloud computing, smart grid, mobile crowdsensing and Internet of Things.

Xiaodong Lin (M'09–SM'12–F'17) received the Ph.D. degree in information engineering from Beijing University of Posts and Telecommunications, Beijing, China, in 1998 and the Ph.D. degree (with outstanding achievement in graduate studies award) in electrical and computer Engineering from the University of Waterloo, Waterloo, ON, Canada, in 2008.

He is currently an Associate Professor with the School of Computer Science at the University of Guelph, Guelph, ON, Canada. His research interests include computer and network security, privacy protection, applied cryptography, computer forensics, and software security.

Xuemin (Sherman) Shen (M'97–SM'02–F'09) received the Ph.D. degree in electrical engineering from Rutgers University, Piscataway, NJ, USA, in 1990.

He is currently a University Professor with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada. His research focuses on resource management in interconnected wireless/wired networks, wireless network security, social networks, smart grid, and vehicular *ad hoc* and sensor networks. He is a registered Professional Engineer of Ontario, Canada, an Engineering Institute of Canada Fellow, a Canadian Academy of Engineering Fellow, a Royal Society of Canada Fellow, and a Distinguished Lecturer for the IEEE Vehicular Technology Society and Communications Society.

Dr. Shen was the recipient of the Joseph LoCicero Award in 2015, the Education Award in 2017, the Harold Sobol Award in 2018, and the James Evans Avant Garde Award in 2018 from the IEEE Communications Society. He was also the recipient of the Excellent Graduate Supervision Award in 2006, and the Outstanding Performance Award in 2004, 2007, 2010, 2014, and 2018 from the University of Waterloo, the Premier's Research Excellence Award (PREA) in 2003 from the Province of Ontario, Canada. He is the Editor-in-Chief for the IEEE INTERNET OF THING JOURNALand the Vice President for the publications of the IEEE Communications Society. He was the Technical Program Committee Chair/Co-Chair for the IEEE Globecom' 16, IEEE Infocom'14, IEEE VTC'10 Fall, the Symposia Chair for IEEE ICC'10, the Tutorial Chair for IEEE VTC'11 Spring, the Chair for IEEE Communications Society Technical Committee on Wireless Communications, and P2P Communications and Networking.

Authorized licensed use limited to: University of Waterloo. Downloaded on July 26,2020 at 19:15:18 UTC from IEEE Xplore. Restrictions apply.