Smart Contract-Driven Mechanism Design to Mitigate Information Diffusion in Social Networks

Arinjita Paul, Vorapong Suppakitpaisarn and C. Pandu Rangan

Abstract This paper presents a new direction in privacy preserving techniques for social networks based on consensus-driven blockchain and mechanism design principles. Privacy problem is among the class of the most important and fundamental problems in social networks. The most commonly accepted privacy solution is to incorporate a perfect data privacy policy and central system, which inherently lacks transparency and trust. All existing privacy techniques deny undesired users access to the information directly, but, in reality, the information may be forwarded to them from other users who possess the information. Our user-controlled privacy mechanism aims to control such data dissemination using simple game theoretic concepts combined with blockchain technology. Our mechanism applies to DAG structured networks (directed acyclic graphs), and our reward policy incentivizes the receivers if they do not diffuse the message in the network. We establish blockchain powered smart contracts to enable the flow of incentives in the system, without the involvement of a trusted third party. The owner of the message has to pay for the rewards, but our mechanism makes sure that the payment is minimum. In fact, the owner will have more utility when he/she pays. Our mechanism satisfies the necessary constraints of mechanism design, namely individual rationality, incentive compatibility, and weakly budget balance while ensuring privacy.

A. Paul (✉) · C. P. Rangan
Department of Computer Science and Engineering, IIT Madras, Chennai, India
e-mail: arinjita@cse.iitm.ac.in

C. P. Rangan
e-mail: prangan@cse.iitm.ac.in

V. Suppakitpaisarn
Graduate School of Information Science and Technology,
The University of Tokyo, Tokyo, Japan
e-mail: vorapong@is.s.u-tokyo.ac.jp

P. Pardalos et al. (eds.), *Mathematical Research for Blockchain Economy*,
Springer Proceedings in Business and Economics,
https://doi.org/10.1007/978-3-030-37110-4_14

1 Introduction

The advent of blockchain technology has led to a paradigm shift from centralised to a decentralised and autonomous control. Blockchain is a decentralised verifiable public ledger which maintains records of transactions in an append-only fashion. Identical copies of the blockchain are distributed among each participating nodes in the network, and any changes to the ledger are reflected across all copies. Initially envisioned for secure transfer of decentralised digital currency [25], the technology has been extended to provide a generalised framework for implementing decentralised applications requiring trusted computing and auditability [35], such as finance, Internet of Things, governance applications, capital markets and e-health [7].

Social networking is pervasive in today's world, leading to a boom in the information economy. Social networking sites have become the preferred medium of information sharing with peers by means of purchases, queries, conversations and other related activities. However, such a popularity has been accompanied by growing concerns for privacy of its users [34]. Such sites form a database of personal data that holds substantial economic value, serving as a hotbed for potential marketing networks, malware, spam, illegal earnings and several other attacks [22, 34] on the Internet. Leakage of critical data such as medical health records and business information regarded as a business asset, could lead to dire consequences such as identity theft, financial loss, harassment and fraud [12]. Social network privacy or informational privacy is still in its infancy, with no well-defined security model. In 2015, medical data of 78.8 million patients, nearly a quarter of the U.S. population, were stolen by a hack on the insurance corporation Anthem as a result of weak policy enforcement and security systems [7].

To address these concerns, social network service providers have developed privacy policies and features [15] to balance the trade-off between privacy threats and data sharing. Note that such privacy measures are traditionally supported by centralized systems, which lack trust and transparency, as evident from the recent breaches in privacy reported in [11, 13].

1.1 Our Contribution

In an attempt to shift from a centralised privacy system to a user-controlled approach, we propose a new direction that employs mechanism design theory combined with blockchain technology to ensure privacy of sensitive data in social networks while improving societal welfare, which hitherto has not been explored in the literature. We propose a novel mechanism, called the Social Network Privacy Mechanism (SNPM), that incentivizes the participants for not diffusing the private information into the network. We leverage blockchain enabled smart contracts [3] as a decentralised approach to automatize the incentive system and tackle trust issues in our privacy mechanism. We prove that our mechanism satisfies all the required properties for a mechanism to function. Those properties are individual rationality, incentive compatibility and weakly budget balance.

We consider the social network as a directed acyclic graph (DAG). Several algorithms for general graphs are obtained from algorithms for DAGs such as [29]. There exist several results that consider social networks with *time label* [17]. Again, temporal social networks can be considered as DAGs [18]. Although it is not straightforward to apply our mechanism to periodic networks, we strongly believe that it could be a possible extension of our mechanism to general graph structures.

1.2 Example

Our mechanism is demonstrated in Fig. 1. A user m wishes to propagate a message only to a set of his neighbours and promises a reward to each receiver who does not propagate the message in the network. To prevent message dissemination, m has a reward amount to incentivize his neighbours (agents a and b here) for not propagating the message. As shown in the figure, user m rewards neighbour b with an amount $R_e = 35$ as an incentive to not propagate his message to user e. Again, user e could bribe user b with a value $B_e = 28$ to acquire the message from b. Since $R_e > B_e$, user b refrains from propagating the message to e, as indicated by red arrows. Our mechanism displays how the reward value is computed by each user in the network, where all financial transactions are performed by a smart contract, to restrict users from message propagation, and demonstrates how equilibrium is attained while preserving message privacy along with the necessary properties of mechanism design.

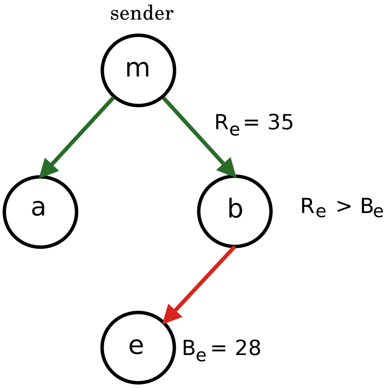

Fig. 1 A social network example to demonstrate our privacy mechanism. A user m shares private information only with users (a, b). The arrows green symbolize message transmission by m to (a, b) and red symbolizes forbidden dissemination to agent e

2 Related Works

2.1 *Integrating Blockchain Technology to Social Networks*

Although the blockchain paradigm was originally designed to maintain a decentralised financial ledger, it has been extended to serve other applications requiring trusted computing and auditability. Recently, several research efforts have focused on blockchain based social networks. This establishes a decentralised approach to connectivity to get rid of a centralised server, preventing any single authority from enforcing monitoring and control over the user generated data for financial incentives. Some examples of decentralised social networks include Akasha [1], Diaspora [8] and Steemit [30] among others. Such principles of decentralization has also been applied for managing large data, such as Ancile [7] and MedRec [2] for electronic health records (EHR) management in a medical network and for personal data [35] management. Note that, one downside of the blockchain technology is that it is resource intensive, and hence scalability is an issue for large scale systems. All existing results rely on the distributed ledger mechanism and external regulations such as the HIPAA privacy rule to address security of individual data. In this paper, privacy of user data is maintained using simple mechanism design principles and the incentives are managed using blockchain. Unlike the previous works stated, the transactions maintained in our ledger are purely financial, to only regulate the financial incentives in the system.

2.2 *Anonymization of Social Networks*

Social Network Anonymization is a countermeasure of linking attack, where undesired users can infer protected information from published data. Such an attack is prevented by removal or perturbation of certain information, while satisfying privacy notions. In relational databases, the most commonly accepted privacy notions include k-anonymity [31], ℓ-diversity [23] or t-closeness [21]. In the context of social network privacy, such notions are extended to concepts such as k-isomorphism [5]. Several graph modification techniques such as graph perturbation [14] and clustering approaches [4] have been introduced, that meet privacy notions for social networks.

Social network anonymization usually addresses privacy problems arising from data publication. On the other hand, we consider a different dimension of information privacy in this work, i.e., preventing private data diffusion in social networks.

2.3 Mechanism Design Towards Social Choices in Networks

In addition to the preference of outcomes of a mechanism (winner in an auction), users may also be concerned with what private information gets leaked to others (the valuation of the auctioned item). The latter notion of privacy has been addressed in the literature using techniques of differential privacy [27, 28]. Informally, differential privacy [10] captures the fact that a change in a single agent's input has too small an effect to jeopardize the privacy and learn any information about the agent from the outcome of a joint computation. Note that, differential privacy offers a compelling second-best solution concept when the exact dominant strategy truthful mechanism is not known [28] as it offers *approximate-truthfulness* [9].

Li et al. [20] applies mechanism design theory to the auction design problem for a seller to sell a commodity in a social network. While their work focuses on increasing the number of users that know the auction information and maximizing the auction bid, our work aims to minimize the number of participants that know the private information. One might think that our mechanism is analogous to the mechanism due to Li et al. However, because of the difference in objectives, the two mechanisms do not share any similarity with each other.

3 Preliminaries

3.1 Blockchain

Blockchain is a distributed ledger technology typically managed by a peer-to-peer network. Its non-trusting members record digital transactions into the shared immutable ledger in a verifiable manner without the need of a centralised regulator. Blockchain implements the concept of *mining* and *proofs* inorder to reach a consensus on the transaction ordering in a decentralized fashion. *Miners* are a subset of the network participants whose role is to validate transactions broadcasted into the network and append these transactions grouped into a *block* to the blockchain. To this end, they fiercely compete with one another to solve difficult computational problems, and are rewarded (usually monetary) for their service. *Proofs* determine which miner's block will be appended next to the blockchain, such as proof-of-work and proof-of-stake. Cryptocurrencies such as Bitcoin [25] and Ethereum [3] are built atop such a technology, wherein the network members run distributed consensus protocols. Recently, there has been an increasing interest to exploit the technology to develop applications beyond digital currencies requiring tamper-proof network consensus. Blockchain has attracted the interest of stakeholders across a wide range of industries owing to its decentralised approach towards providing trust and integrity in the network, such as healthcare, real estate, finance, cloud storage, governance applications among others.

3.2 Smart Contracts

Introduced in 1994 by Nick Szabo, a smart contract is “a computerized transaction protocol that executes the terms of a contract” [32]. It is a user defined software executed by a network of mutually distrustful parties, and has received much attention in the context of blockchains. Its correct execution is automatically enforced without the arbitration of any central authority, and stores its result on the blockchain. One such example of smart contracts are Ethereum [3], which builds a Turing-complete instruction set to allow smart contract programming into the blockchain, and records the contract states on the blockchain. Depending on the intended application, smart contracts could be used towards financial, notarial or game-based applications among others. Since such scripts are tamper resilient and their actions are publicly visible, they are appealing in scenarios that require transfer of money to respect certain agreed rules. We regard such a feature offered by smart contracts as an important property to achieve financial fairness in our privacy mechanism.

3.3 Mechanism Design

Mechanism design is a fundamental concept in economics and AI [26]. It is an art of creating economic interactions with respect to a preferable outcome of the game induced by the mechanism. We closely follow the mechanism design framework in [24]. We consider a social network consisting of n persons or agents represented by a set N, where each agent is indexed by $i \in \{1, \dots, n\}$. Every agent $i \in N$ must report its action $a_i \in A_i$ for the public decision, where A_i denotes the complete action space of an agent i possible towards social welfare. Let $a = (a_1, a_2, \dots a_n)$ be a vector that denotes the action profile of all the agents $i \in N$, and A denotes the complete action space for all agents in the network. We use the following notation N_{-i} to denote the set $N \setminus \{i\}$ which is the set of all agents except agent i, and the notation a_{-i} to denote the action profile of all agents except agent i.

In the auction setting, every agents bid for a number of objects. For simplicity, in this paper, we will assume that the number of objects is one. Every agent $i \in N$ has a value of the object $v_i \in \mathbb{R}$ that indicates his willingness or valuation on that object. The agents then take an action to report how much they want to pay for the bid. By that, the action set A_i denotes the set of all possible report values. Let $\pi_i(a)$ be a decision function of the mechanism where $\pi_i(a) = 1$ when the agent i is a winner who can receive the object and $\pi_i(a) = 0$ otherwise. The winner i will then have to pay an amount equal to p_i for the object to the auctioneer. In the most well-known Vickrey mechanism [33], the winner is the agent that report the largest value, i.e. $pi_i(a) = 1$ if and only if $a_i = \max_{j \in N} a_j$, and the price that she has to pay is equal to the second largest value, i.e. $p_i = \max_{j \in N_{-i}} a_j$. The utility of the agent i, denoted by $u_i(a)$ is then computed as $u_i(a) = \pi_i(a) \cdot (v_i - p_i)$.

Given the basic definitions, we formalize the desirable three criteria for evaluating a mechanism, which are *individual rationality*, *incentive compatibility* and *weakly-budget balanced.*

Since every agent a_i is rational, their action a_i is in the selfish interest to maximize their individual utilities $u_i(a)$. She might bid with the values larger or smaller than her evaluation on the object. That usually lead to a smaller social welfare $\sum_{i=1}^{n} u_i(a)$. If a mechanism is individually rational, the agent can be sure that reporting a honest value, $a_i = v_i$ in the auction mechanism, never lead to a negative utility.

Definition 1 A mechanism is individually rational if $u_i(v_i, a'_{-i}) \geq 0$ for all $i \in N$, and $a'_{-i} \in A_{-i}$.

The incentive compatibility then guarantees that reporting the honest value will lead to the maximum utility.

Definition 2 A mechanism is incentive compatible if $u_i(v_i, a_{-i}) \geq u_i(a_i, a'_{-i})$ for all $i \in N, a_i \in A_i$ and $\{a_{-i}, a'_{-i}\} \in A_{-i}$.

Next, we will define the notion of weakly-budget balance.

Definition 3 A mechanism is weakly-budget balanced if the payment policy p does not exhibit a budget deficit for a utility profile u, i.e.,

$$\sum_{i=0}^{n} p_i \geq 0$$

Note that $\sum_{i=0}^{n} p_i$ is a sum of all agents' payment in the network. The intuition for a mechanism to be weakly-budget balanced is that, in case of a negative revenue, a payment made by agents is not covered by the payment received by the agents in the network. Besides, there is no external source to finance the mechanism to function and provide an outcome.

4 Social Network Privacy Mechanism (SNPM)

In this section, we design a mechanism to conquer the problem of privacy in social networks, which we call Social Network Privacy Mechanism (SNPM). We show that our mechanism satisfies all the necessary properties, i.e., it is individually rational, incentive-compatible and weakly budget balanced. First, we give an overview of our model, to demonstrate the setting on which we enforce social network privacy.

4.1 Our Model

In our model, each agent $i \in N = \{1, \ldots, n\}$ in the social network has a set of neighbours denoted by $d_i \subseteq N$, with whom the agents can communicate directly via the link/edge. An agent termed as messenger $m \in N$ has a private message and wishes to propagate the message to only a selected set of neighbours and discourage them from further propagating to other agents in the network. Every agent in the network is oblivious of the presence of other agents except his neighbours. In our model, the messenger is not aware of the network structure beyond its neighbours.

We consider that the information diffusion flow in the network forms a direct acyclic graph (DAG). Such an assumption is reasonable, evident from the existing results in the social network literature [19], and extensions of algorithms on DAGs to general graph structures [29]. There exists algorithms for conversion of periodic graphs to DAGS [6], which could be a possible albeit challenging extension of our mechanism to incorporate generic network structures.

In order to achieve a decentralised, permanent and uncensorable mode of payment, we use blockchain systems like Ethereum [3] and NEO [16], wherein every agent joins the network (generates a unique identifier for each agent) and can access all the transactional information on blockchain. Such a system maintains a log of transactions of the agents via smart contracts. It relies on the multiple participating entities in the system to avoid a single-point-of-failure and single-point-of-breach. This makes the business model and incentive structure much robust and trusted, instead of assuming the presence of a trusted authority. Our main idea is to reward the agents who do not propagate the message. To this end, the messenger intends to reward amount values U_i for every agent $i \in N_{-m}$, allocated based on the preferences of message sharing of the messenger. All the reward and bribe transactions are automated through smart contracts.

U_i denotes the benefit of the messenger if the message is not propagated to agent i. The utility of the messenger will increase by $U_i \geq 0$ if the agent i do not receive the message. On the other hand, every agent $i \in N_{-m}$ maintains a valuation v_i for the message propagated by the messenger. The utility of the agents $i \in N_{-m}$ increases by a value $v_i \geq 0$ on acquiring the information. Agents who do not receive the message from m may bribe their neighbours with an amount $v_i' \leq v_i$ to acquire the message. Again, the messenger rewards the non-propagating nodes (via smart contracts) with a reward value $r_i \leq U_i$ for not propagating the message. Hereon, we consider all the transactions between the messenger and the agents are automated by smart contracts.

In our model, the action of every agent i is denoted as a tuple $a_i = (v_i', d_i')$. The value $v_i' \leq v_i$ is the bribe i pays to a neighbour who receives the message. The set $d_i' \subset d_i$ is the set of neighbours (descendants) to whom i spreads the message on receipt of bribe. The action space A_i is $V_i \times \mathcal{P}(d_i)$ where V_i represents the set of real number no larger than v_i and $\mathcal{P}(d_i)$ represents the power set of the neighbour set d_i.

Our decision function is represented by $\pi_i : A \rightarrow \{0, 1\}$, where $\pi_i(a) = 1$ if agent i is allocated the message due to the action a, and $\pi_i(a) = 0$ otherwise. Therefore, we denote the set $\pi = \{\pi_i\}_{i \in N_{-m}}$ as an *allocation policy* in this work.

The motive of every agent i is to acquire the message and their action a_i are in the selfish interest to maximize their individual utilities while receiving the message. Therefore, the agents could misreport their valuations (bribe) of the message. A privacy mechanism is *individual rational* if the utility of an agent reporting true valuations is not negative.

A mechanism is *incentive compatible*, if reporting the true valuations by the agents in the mechanism is a dominant strategy.

The revenue generated by the mechanism is calculated as a sum of the payment balance between the messenger and other agents in the network in an action profile. The reward sum of the messenger equals $Rev_m(a) = \sum_{i \in N_{-m}} r_i$, while every agent $i \in N_{-m}$ pays their neighbours a sum equal to $Rev_i(a) = \sum_{i \in N_{-m}} p_i$. The total revenue for an action profile must be non-negative, to avoid shortage of budget in order that the mechanism is *weakly budget balanced*. It is easy to follow that the revenue generated by our mechanism $Rev_i(a) = \sum_{i \in N} p_i = 0$. For all agents $i \in N_{-m}$, the reward value r_i paid by the messenger to the agent i and the bribe sum $v_j, \forall j \in d_i'$ is annulled by the payment p_i made by the agent i in the overall revenue, thereby resulting in a zero sum.

4.2 Our Mechanism

Given our model, we next propose our mechanism for social network privacy. An overview of our mechanism is shown in Fig. 2. We design a recursive strategy to define our privacy mechanism. We use the following notations. Let B_i denote the total bribe amount that agent $i \in N_{-m}$ can offer to its neighbour who possesses a message. Let R_i denote the total reward amount of the messenger m for an agent i,

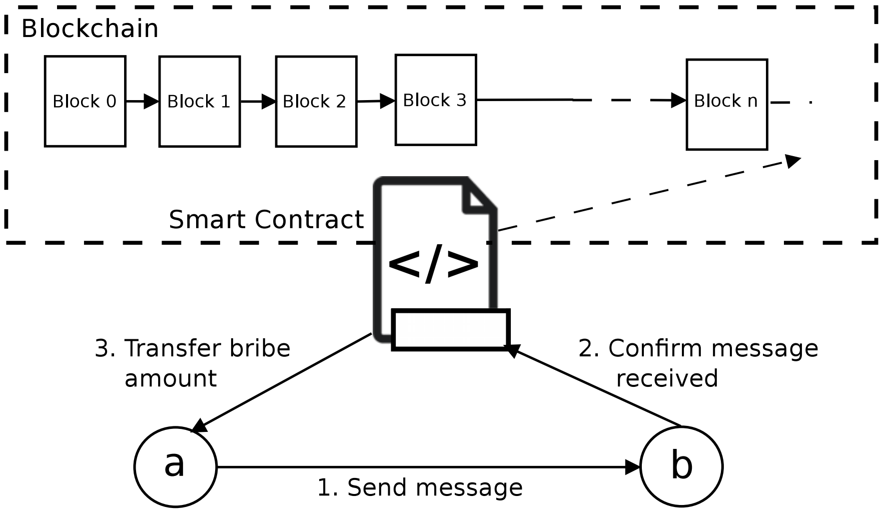

Fig. 2 Overview of SNPM. In the example, if agent a can acquire a higher amount of bribe B_a from agent b than the reward R_a, it sends the message to agent b. On receiving the message, the smart contract confirms the message receipt from b, and transfers the bribe amount from agent b to agent a and records on the blockchain

sufficient to stop i from receiving a bribe. Therefore, the total bribe i can pay for a message is the sum of the bribe received from his neighbour set d_i' along with his own bribe amount v_i. Therefore, every agent i can compute its budget as below:

$$B_i = v_i + \sum_{j \in d_i', U_j \geq v_j} (B_j + \epsilon) + \sum_{j \in d_i', U_j < v_j} (R_j).$$

The above formula defines a recursive structure for the computation of the total budget of an agent in order to bribe his neighbour possessing the message. Every agent can pay a bribe value equivalent to the bribe sum of its descendants. Also, the reward sum R_i for a messenger is the sum of the messenger's utility for all the descendants of a non-propagating agent.

The reward amount R_i of the messenger m is the collective utility of m if agent i does not receive the message (utility is U_i) and the utility of its descendants (utility is $U_j, \forall j \in d_i'$), minus the total reward value paid by m if i along with its descendant agents receive the message and do not propagate it to their descendants. We denote the collective utility as $\mathbb{U}_i$ and the cumulative reward as $\mathbb{R}_i$. Let $(\mathbb{U}_i)_{without}$ denote the collective utility of the messenger when agent i does not receive the message, and $(\mathbb{U}_i)_{with}$ to denote the same when i receives the message. Similarly, let $(\mathbb{R}_i)_{without}$ denote the collective reward for agent i when it does not receive the message, and $(\mathbb{R}_i)_{with}$ to denote the same when i receives the message. From the concept of VCG, the total reward amount of the messenger to offer agent i is computed as below:

$$\begin{aligned}
R_i &= (\mathbb{U}_i)_{without} - (\mathbb{R}_i)_{without} - ((\mathbb{U}_i)_{with} - (\mathbb{R}_i)_{with}) \\
&= (\mathbb{U}_i)_{without} - 0 - (\mathbb{U}_i)_{with} + (\mathbb{R}_i)_{with} \\
&= U_i + \sum_{j \in d_i'} (\mathbb{U}_j)_{without} + \sum_{\substack{j \in d_i', \\ U_j \geq v_j}} (B_j + \epsilon) \\
&= U_i + \sum_{\substack{j \in d_i', \\ U_j < v_j}} (R_j) + \sum_{\substack{j \in d_i', \\ U_j \geq v_j}} (B_j + \epsilon).
\end{aligned}$$

Note that, in the above derivation, $(\mathbb{U}_i)_{without}$ is the utility of the messenger when agent i does not receive the message, which is U_i. Also, $(\mathbb{R}_i)_{without} = 0$ since an agent i who does not possess the private message will not be rewarded as per the mechanism. Given the scenario, the motive of the mechanism is to convince an agent possessing the message to not accept bribe with the reward value. Naturally, for an agent i, if $R_i > B_i$, the agent is motivated to not receive any bribe from its descendants. Now we propose our mechanism based on the above definitions.

Definition 4 (*Privacy Mechanism SNPM*) Given the action profile a of the agents, the privacy mechanism SNPM is defined by an allocation policy π and a payment policy p, which are defined as follows.

The allocation policy of the privacy mechanism is defined as:

$$\pi_i(a) = \begin{cases} 1, & \text{if } B_i \geq R_i \\ 0, & \text{otherwise} \end{cases}$$

Note that, there could exist multiple agents who are allocated the message, that is, multiple agents with sufficient $B_i \geq R_i$ have the budget to bribe agents to acquire the message, which also represents the subset of users for whom m does not have enough reward to stop propagation. There exists a reward policy, which is the incentive given by the messenger to the agents who do not diffuse the message to his descendants. The reward policy of the privacy mechanism is defined as:

$$r_i(a) = \sum_{j \in d_i'} (1 - \pi_j)(B_j + \epsilon).$$

Assume that under the allocation policy, an agent i gets the message, the payment policy is defined as follows:

$$p_i = B_i - \sum_{j \in d_i'} \pi_j(a) \cdot R_j - r_i(a)$$

The privacy mechanism allocates the message to all the agents whose bribe amount B_i is greater than R_i. The smart contract consists of the function to confirm the receipt of message from those agents i and transfer the bribe amount B_i to the bribed agents. Each agent makes a net payment equal to his bribe value, minus the bribe amount received from all his descendants. Note that if an agent $i \in N$ could potentially receive the message from $c > 1$ number of agents possessing the message, then bribe value v_i of the agent i is equally distributed to all c agents by the smart contract. Similarly, if multiple agents do not receive bribe from a common descendant i, the reward value r_i is equally divided among the honest agents in our mechanism.

4.3 Example

Before analyzing the properties of our privacy mechanism SNPM, we study an example given in Fig. 3 to demonstrate our mechanism. Figure 3a shows a simple social network, where each node represents an agent, and m denotes the messenger who wishes to propagate the message to a subset of agents in the network. The edges between the nodes represent the neighbourhood relationship. The values provided alongside the nodes represent the valuations associated with each agent in the form of U_i/v_i, i.e., the first value represents the messenger valuation U_i and the value v_i represents the agent's valuation for the message. In this setting, we assume that all the agents truthfully report their valuations. Suppose the messenger wishes to propagate

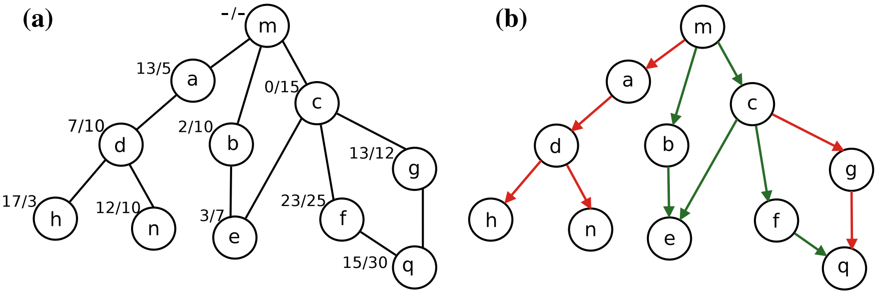

Fig. 3 **a** A social network example depicting the utilities of messenger/agents for a message forwarded by agent m. **b** The corresponding information diffusion network

a private message only to a subset of his neighbours in the network, i.e., agents b and c. The agent b has one descendant e and agent c has three descendants e, f and g who could potentially bribe b and c respectively for the private information. The recursive equation to obtain the cumulative bribe amount and reward for agents b and c is computed as follows:

$$R_b = U_b + \frac{1}{2}R_e.$$

$$B_b = v_b + \frac{1}{2}R_e.$$

$$R_c = U_c + R_f + (B_g + \epsilon) + \frac{1}{2}R_e.$$

$$B_c = v_c + R_f + (B_g + \epsilon) + \frac{1}{2}R_e.$$

We note that, as per our definition, both the agents b and c are potential sources of the private information for agent e, and hence the bribe value of e is equally distributed to both b and c. We recursively compute the same for the descendants e, f and g as follows:

$$R_f = U_f + \frac{1}{2}R_q.$$

$$B_f = v_f + \frac{1}{2}R_q.$$

$$R_g = U_g + \frac{1}{2}R_q.$$

$$B_g = v_g + \frac{1}{2}R_q.$$

The agent e have $R_e = U_e = 3$, $B_e = v_e = 7$ and $\pi_e = 1$. Similarly, agent q has $R_q = 15$, $B_q = 30$ and $\pi_q = 1$. Solving the recursive equations, we obtain $R_f = 30.5$, $B_f = 32.5$ and $\pi_f = 1$. Again, $R_g = 20.5$, $B_g = 19.5$ and $\pi_g = 0$. Finally, the net budget for agents b and c obtained is $R_b = 3.5$, $B_b = 11.5$ and $\pi_b = 1$, again $R_c = 51.5 + \epsilon$, $B_c = 66.5 + \epsilon$ and $\pi_c = 1$. Hence, agents e, f and q successfully receives the message by bribing via the smart contract as illustrated by the information diffusion network in Fig. 3b. In the figure, the green arrows denote the information diffusion flow, and the red arrows denote the forbidden flow to unintended agents. The budget of node g is not sufficient to bribe his neighbours c or q for the message, and hence he is forbidden from the message. As per the payment policy, the payment made by the agents e, q and f towards bribing their neighbours are $p_e = 7$, $p_q = 30$ and $p_f = 25$ respectively.

4.4 Properties

Theorem 1 The Social Network Privacy Mechanism is individually rational.

Proof Assume that an agent $i \in N_{-m}$ truthfully reports her bribe $v_i' \leq v_i$ to receive the message. If $v_i' > U_i$, agent i receives the message and her utility $u_i(a_i, a') > 0$, while if $U_i > v_i'$, the agent i does not receive the message and his payment due is zero according to the payment policy. If an agent i reports a bribe $v_i' > v_i$ such that $U_i < v_i'$, according to the allocation policy $\pi_i = 1$ and he receives the message. However his utility $u_i = (v_i - v_i') - p_i$ is negative. Therefore, for an arbitrary agent, when he truthfully reports her bribe, his utility is non-negative and SNPM is individually rational.

Theorem 2 The Social Network Privacy Mechanism is incentive compatible.

Proof To prove that SNPM is incentive compatible, we analyze the action of all the agents in the social network in the following two cases:

Case 1: If an agent $i \in N$ is forbidden from receiving the message, it indicates that $R_i > B_i$ and $\pi_i = 0$ according to the allocation policy. For any agent j who is a potential source of the message for node i, agent j receives an reward $B_i + \epsilon$ for not receiving a bribe from agent i, whereas it receives a lesser bribe value B_i from agent i. Therefore, agent j has no motivation in receiving a bribe from its descendant i as it does not maximize his utility. Hence, not propagating the message is a dominant strategy for an agent j whose descendant i exhibits $R_i > B_i$.

Case 2: If an agent $i \in N$ has sufficient budget to bribe an agent for receiving the message, it indicates that $R_i < B_i$ and $\pi_i = 1$ according to the allocation policy. For any agent j, who is a potential source for the message to node i, agent j receives an reward R_i for not receiving a bribe from agent i, whereas it receives a higher bribe value $B_i > R_i$ from agent i. Therefore, agent j has no motivation for stopping a message propagation to descendant i in return of a bribe value B_i, as it maximizes his utility. Hence, propagating the message is a dominant strategy for an agent j whose descendant i exhibits $R_i < B_i$ and is eligible to receive the message.

Therefore, for an agent $i \in N$ possessing the private message, propagating the message to only those agents who pay a higher bribe value than the reward offered and not propagating to the forbidden descendants is a dominant strategy. This ensures incentive compatibility for SNPM.

We note that the SNPM mechanism is *weakly budget balanced* which follows from the discussion in Sect. 4.1.

5 Conclusions and Future Work

In this paper, we generalized the mechanism design problem to the social network privacy setting, in which a sender sends a private message to a selected list of agents in the network, propagated to other agents through the neighbours of the sender. Our mechanism promotes message privacy by leveraging blockchain powered smart contracts to incentivize the receivers who do not disperse the message to their neighbours. Our privacy mechanism is novel in the sense that it employs simple game theoretic tools and distributed consensus mechanism to employ privacy in the social network, while satisfying all the necessary conditions for a mechanism to function. Our mechanism can function in a network involving multiple message propagation from multiple senders, as each message sharing is independent of the other, and does not create any conflict the system. The previous attempts to ensure privacy of user data in social networks were mainly achieved through centrally enforced policies and privacy systems that lacks trust and transparency, or employing a public ledger based distributed networking system to track private data, which suffers from scalability issues. Our approach positively resolves the problem of shared data privacy by employing simple albeit significant mechanism design principles.

We assume the underlying diffusion network to be a directed acyclic graph (DAG). The existence of algorithms for conversions of periodic structures to DAGs creates the possibility (although challenging) of an extension of our algorithm to generic graph structures. We leave it as an open problem. In addition to that, we plan to integrate time to our mechanism. That will decrease the possibility that our game may continue forever.

It would also be an interesting direction to efficiently incorporate mechanism design and blockchain technology in other aspects of privacy preservation in social networks, such as anonymization and privacy preservation of user information.

Acknowledgements Parts of this work is done while Arinjita Paul was conducting an internship supported by the JST Sakura Science Program. We would like to thank Prof. Satoru Iwata for hosting the internship. We also would like to thank anonymous reviewers who give comments that can significantly improve this paper.

References

1. Akasha: http://akasha.world/ (2015)
2. Azaria, A., Ekblaw, A., Vieira, T., Lippman, A.: Medrec: using blockchain for medical data access and permission management. In: 2nd International Conference on Open and Big Data, OBD 2016, Vienna, Austria, 22–24 August 2016, pp. 25–30 (2016)
3. Buterin, V., et al.: A next-generation smart contract and decentralized application platform. White paper (2014)
4. Casas-Roma, J., Rousseau, F.: Community-preserving generalization of social networks. In: Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, ASONAM 2015, Paris, France, 25–28 August 2015, pp. 1465–1472 (2015)
5. Cheng, J., Fu, A.W.-C. Liu, J.: K-isomorphism: privacy preserving network publication against structural attacks. In: Proceedings of the 2010 ACM SIGMOD International Conference on Management of data, pp. 459–470. ACM, New York (2010)
6. Cohen, E., Megiddo, N.: Recognizing properties of periodic graphs. In: Applied Geometry and Discrete Mathematics, Proceedings of a DIMACS Workshop, Providence, Rhode Island, USA, 18 September 1990, vol. 4, pp. 135–146. DIMACS/AMS (1990)
7. Dagher, G.G., Mohler, J., Milojkovic, M., Marella, P.B.: Ancile: privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustain. Cities Soc. **39**, 283–297 (2018)
8. Diaspora: https://diasporafoundation.org/ (2010)
9. Dwork, C.: The differential privacy frontier. In: Proceedings of Theory of Cryptography, 6th Theory of Cryptography Conference, TCC 2009, San Francisco, CA, USA, 15–17 March 2009, pp. 496–502 (2009)
10. Dwork, C., McSherry, F., Nissim, K., Smith, A.D.: Calibrating noise to sensitivity in private data analysis. In: Proceedings of Theory of Cryptography, Third Theory of Cryptography Conference, TCC 2006, New York, NY, USA, 4–7 March 2006, pp. 265–284 (2006)
11. Goel, V.: Facebook tinkers with users emotions in news feed experiment, stirring outcry. The New York Times (2014)
12. Gradwohl, R.: Information sharing and privacy in networks. In: Proceedings of the 2017 ACM Conference on Economics and Computation, EC '17, Cambridge, MA, USA, 26–30 June 2017, pp. 349–350 (2017)
13. Hardekopf, B.: The big data breaches of 2014. Forbes, 13 January 2015
14. Hay, M., Miklau, G., Jensen, D., Weis, P., Srivastava, S.: Anonymizing Social Networks. Computer Science Department Faculty Publication Series, p. 180 (2007)
15. Henson, B., Reyns, B.W., Fisher, B.S.: Security in the 21st century: examining the link between online social network activity, privacy, and interpersonal victimization. Crim. Justice Rev. **36**(3), 253–268 (2011)
16. Hongfei, D., Zhang, E.: https://docs.neo.org/en-us/whitepaper.html (2014)
17. Iwano, K., Steiglitz, K.: Testing for cycles in infinite graphs with periodic structure. In: Aho, A.V. (eds.) Proceedings of the 19th Annual ACM Symposium on Theory of Computing, pp. 46–55. ACM, New York (1987)
18. Kempe, D., Kleinberg, J.M., Kumar, A.: Connectivity and inference problems for temporal networks. In: Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing, Portland, OR, USA, 21–23 May 2000, pp. 504–513. ACM, New York (2000)
19. Kleinberg, J.M., Raghavan, P.: Query incentive networks. In: Proceedings of 46th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2005), 23–25 October 2005, Pittsburgh, PA, USA, pp. 132–141. IEEE Computer Society (2005)
20. Li, B., Hao, D., Zhao, D., Zhou, T.: Mechanism design in social networks. In: Proceedings of the Thirty-First AAAI Conference on Artificial Intelligence, San Francisco, California, USA, 4–9 February 2017, pp. 586–592 (2017)

21. Li, N., Li, T., Venkatasubramanian, S.: t-closeness: privacy beyond k-anonymity and l-diversity. In: IEEE 23rd International Conference on Data Engineering. ICDE 2007, pp. 106–115. IEEE (2007)
22. Luo, W., Liu, J., Liu, J., Fan, C.: An analysis of security in social networks. In: Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, pp. 648–651. IEEE (2009)
23. Machanavajjhala, A., Gehrke, J., Kifer, D., Venkitasubramaniam, M.: l-diversity: privacy beyond k-anonymity. In: Proceedings of the 22nd International Conference on Data Engineering. ICDE'06, pp. 24–24. IEEE (2006)
24. Moulin, H.: Axioms of Cooperative Decision Making. Econometric Society Monographs, vol. 15. Cambridge University Press, Cambridge (1991)
25. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system (2008)
26. Nisan, N., Roughgarden, T., Tardos, E., Vazirani, V.V.: Algorithmic Game Theory, vol. 1. Cambridge University Press, Cambridge (2007)
27. Nissim, K., Smorodinsky, R., Tennenholtz, M.: Approximately optimal mechanism design via differential privacy. In: Innovations in Theoretical Computer Science, Cambridge, MA, USA, 8–10 January 2012, pp. 203–213 (2012)
28. Pai, M.M., Roth, A.: Privacy and mechanism design. SIGecom Exch. **12**(1), 8–29 (2013)
29. Rajagopalan, K.: Interacting with users in social networks: the follow-back problem. Technical report, MIT Lincoln Laboratory Lexington United States (2016)
30. Steemit social network: https://steemit.com/ (2016)
31. Sweeney, L.: k-anonymity: a model for protecting privacy. Int. J. Uncertain. Fuzziness Knowl.-Based Syst. **10**(05), 557–570 (2002)
32. Szabo, N.: Smart contracts (1994)
33. Vickrey, W.: Counterspeculation, auctions, and competitive sealed tenders. J. Financ. **16**(1), 8–37 (1961)
34. Williams, J.: Social networking applications in health care: threats to the privacy and security of health information. In: Proceedings of the 2010 ICSE Workshop on Software Engineering in Health Care, pp. 39–49. ACM, New York (2010)
35. Zyskind, G., Nathan, O., Pentland, A.: Decentralizing privacy: using blockchain to protect personal data. In: 2015 IEEE Symposium on Security and Privacy Workshops, SPW 2015, San Jose, CA, USA, 21–22 May 2015, pp. 180–184 (2015)