Discussion about an anonymous and trusted communication environment

Discussion about an anonymous and trusted communication environment

Akihiro Fujii
Dept. of Applied Informatics, Hosei University, Tokyo, Japan

***Abstract*: Currently, common publication and communication environments are provided by large private service providers, so-called "platformers". They are basically operated based on commercial and marketing principles. In the environment, a writer is vulnerable to unfair denial of service attacks by a group people with confronting opinions, since the opportunity for the publication is controlled by the platformer's regulations. In this paper, the possibilities of a trusted communication environment using blockchain technology is discussed. We assume several distributed managers (DMs) issuing accounts of users, which follow minimal regulation to keep anonymity and fair activities of participants. Firstly, the double issuing of accounts from a single user is prohibited and supervised by a blockchain mechanism. Secondly, activities such as publishing, evaluations, recommendation, citation and so on are operated fairly with an allocated number of points. The amount of points is maintained by the blockchain mechanism as well. We discuss the realizability and feasibility of such a system from the points of view of fairness and anonymity.**

I. Introduction

In this paper, we discuss issues related to anonymity and fairness in terms of web-based distributed system architecture. The web-based information system can create an open communication space for everyone based on the Internet. The motivation of this paper is to discuss whether current IT technological elements, such as blockchain in distributed web systems can cope with the issues of anonymity and fairness in forming a community with a variety of opinions and diversity of political stances. Currently common publication and communication environments are provided by large service providers, so-called "platformers." They are basically operated based on commercial principles meaning that the providers profits come from sponsors which cover the cost of the system. Those service providers set their own regulations for the publication of users. Let us show a recent non-rare example of an unfair incident on SNS which happened in Japan. Once a journalist published an article about a controversial issue, a group of users who disagreed with the opinion cast claims to the platform administration directly without discussing the issue in the communication space. They claimed that the publication was inappropriate and against the regulation, in order for the account of the journalist to be banned by the service provider. Even though the journalist's publishing was decent and the issue is worth discussing among participants with a variety of opinions, those distorted users with extreme attitudes can ban the utilization of the communication space of another participant. Since the communication space is provided for free to a majority of ordinary users, they must obey the sanction made by the platform provider. As a consequence, the common SNS communication environment is vulnerable for such organized denial of service attacks. In recent years, distributed ledgers such as blockchain have been applied to a variety of services including electric voting[1][2][3]. The technology has potential to cope with the issue mentioned above.

In this paper, we discuss the possibility to construct an anonymous and fair communication environment using the blockchain mechanism. After some surveys in II, the basic structure is introduced in III. In IV and V, further implementation issues are discussed. A web API (application programming interface) with semantic web technology is considered to provide solutions for achieving the proposed features over a cloud computing environment. The concluding remarks in VI give some drawbacks and future possibilities of the research.

II. Related works and Viewpoints of discussion

A. *SNS Service as a Communication Space*

In this section, some related references are introduced in terms of building anonymous and fair publishing as well as a communication environment over the common internet. For the issue related to anonymity, schemes for identity escrow are proposed in [6] and [10]. They mainly focus on membership management and, as a use-case scenario, an online discussion community with the schema is discussed. As an example of fair maintenance of individual data, a secure voting mechanism is discussed in [7]. There, each vote is treated as single block of data. The P2P (Peer-to-peer) network allows communications only between two previously connected peers. This scheme possibly avoids man-in-middle attacks so that the fairness of voting is assured since the distributed ledger of the blockchain does not allow mass updating of data at a time. In [8], blockchain technology is applied to make a safe and anonymous communication environment for political refugees. Those vulnerable people may need communication means to a separated family member without disclose their identities in escaped countries. This paper is inspired by those examples.

B. *Discussion Standpoints in This Paper*

Since we treat this issue from a technology management point of view, discussions are in the following standpoints.

(a) Ethical and political issues are excluded from the discussion.

(b) Practical implication issues such as choice of existing blockchain platforms, like *Ethereum*, is out of the paper's focus.

(c) Although there are variety of attacks that should be considered in the design of the system, technological discussions are limited to how to achieve anonymity and fairness over the communication environment.

III. The Basic Structure

In this section, the basic structure of the system to support the communication environment is described. The system consists of several distributed entities, namely distributed managers (DMs), and participants take part in the communication environment through the admitted accounts issued by the DMs. In the following, the implementation of each layer is discussed.

A. *The Basic Structure of the Proposed System*

When we construct web applications nowadays, adopting a cloud computing environment is the default scheme. Basically, there are three types of utilizations, SaaS, PaaS, and IaaS. We assume that the system is constructed over PaaS (platform as a service) that common IT service providers such as AWS, GCP or Azure could support. We assume the system consists of several distributed managers, DMs for short, that are in charge of user management and blockchain data management. For constructing a DM system, a standard operating system with internet access, such as Ubuntu, is required. Over those multiple distributed platforms, the proposed communication environment is constructed as SaaS (software as a service) applications.

The system is designed by a layered structure. The three-layered architecture is assumed over a common PaaS environment of a cloud computing service. The functions to achieve in each layer is shown in Table 1. Each layer is considered to provide a set of functions for the upper layer and so forth. The 1st layer provides circulation of the distributed ledger of a blockchain in which participants' account information is recorded. The 2nd layer provides participants' point circulation mechanism also based on the distributed ledger of a blockchain. In the 3rd layer, as an application, fair publications are available. In the following sections, features are explained consequently.

TABLE I. Role of each Layer

Layer	Roles of Distributed Manager	Services for Participant
3	Publication Reputation management, Ranking service	Publication Recommendation Point exchange
2	Distributed ledger of points management	Account issuing Point allocation
1	DM: Distributed Manager Byzantine Algorithm issuing user accounts	
PaaS in Cloud Computing over the Internet		

The DMs are operated by different organizations possibly with confronting business or political stances. At least, they agree with minimum federal regulations. The picture in Fig. 1 depicts the relationship between DMs and users. The role of a DM is primally to avoid double-issuing on an user, then to ensure fair and anonymous activities for the users in the communication space. Hereinafter in this paper, the word 'participants' indicate such users. We will discuss how to achieve such operations over DMs in the later sections.

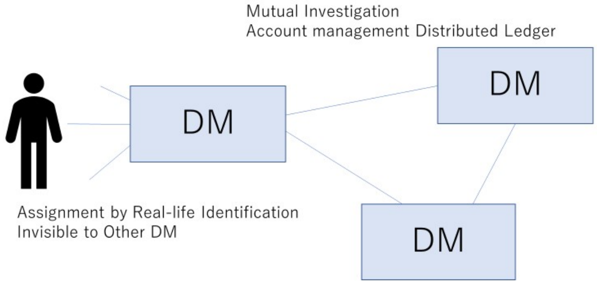
Mutual Investigation
Account management Distributed Ledger
DM
DM
DM
Assignment by Real-life Identification
Invisible to Other DM

Fig. 1. Distributed Managers

B. *Blockchain as Distributed Ledger*

Here, for convenience in the later discussion, we give a short explanation about distributed ledger with blockchain mechanism. We apply blockchain technology for two different level of operations, one is for anonymity in accounts issued in Layer 1. The other is for the fairness management of evaluations of publication by participants in Layer 2. Before discussing them, we briefly review the basic features of blockchain here. The blockchain handles hashed data frames among several distributed sites. A significant aspect is that the system does not require a central controlling mechanism. Each system treats a data frame which is processed by one directional mapping functions called the hash function. As a result, the sequence of past records of transactions written in the frame can never be changed afterwards along with the timeline. When a distributed member circulates this data frame through the communication network, the order of data transmission is uniquely maintained among them. The level of security of the system depends on the model of assumed behaviors of distributed entities. There are three models of assumptions, fail-stop, fail-recover, and Byzantine-faults. There are well-established software libraries available. Some examples are, Ethereum and Hyperledger Fabric. In this article we avoid detailed discussion of the choice of model behavior and algorithm. Here the necessary assumption is that the account information of participants and associated profile information can be maintained with forgery-proof by using blockchain. In the later section, we explain how to apply this technology.

C. *Anonymity Maintainance*

We discuss anonymity from two orthogonal aspects. One is hiding real-life identification, and the other is avoiding double issuing of user accounts to the system. For the sake of discussion, we use term 'anonymity' for hiding one's identification and 'double-counting' for avoiding multiple user accounts. In fact, we are not completely confident about both. The operation of common communication environments is based on the regulations of the SNS. There may be a risk of distortion or monopolization of the platform.

At first, we touch upon anonymity. In the previous research, for example in [6] and [10], three levels of anonymity are defined. Those are 'identity', 'pseudonymity', and 'anonymity'. In any kind of service that is provided with issuing accounts, one should disclose one's identification to the service provider. We assume the existence of a preemptive organization which is probably run by the public sector. They are authorized for user to escrow identity and to issue pseudonymous ID, so called p-ID. The local government might be an appropriate body to play the role of issuing p-ID. By using p-ID, a secondary organization issues 'handling ID', say 'h-ID', which is used when participants write and read articles in the communication environment. In our proposal, DMs play the role of this secondary organization. Once p-ID is issued in preemptive organization, it is theoretically possible to make registration without exposing any personal information to the DM, so that anonymity is ensured. The basic relations are described in Fig. 2.

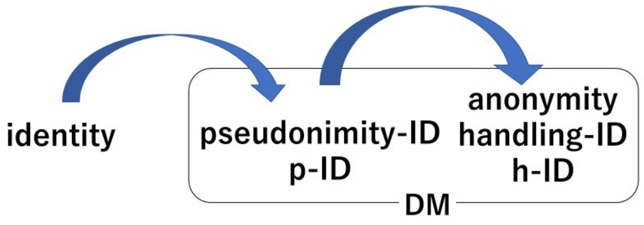

Fig. 2. Idendification escrow in a DM

Now let us name the collection of DMs 'federation'. We propose that the federation keeps the list account information of p-ID/h-ID references consistently with distributed ledger. We assume that every DM is faithful to the minimal regulations to keep the distributed ledger in which account information is recorded. In the federation, the preemptive organization which issued p-IDs from identity should be included. Consequently, double counting is avoided.

D. *Layer 1*

In order to improve confidentiality to both anonymity and double-counting, we assume every DM exchanges the list of accounts every time a new participants joins or leaves the system, The list is managed with a blockchain ledger that may reduce the risk of monopoly over account management. If we introduce a Byzantine algorithm for the management of user membership, the risk of fraud operations is further reduced.

E. *Layer 2*

In Layer 2, the point allocation is performed based on participants' profiles. The profile includes the history of published articles and recommendation messages to the published articles by the participants. This shows one's activity in the communication space. For the profile, the data format should also be maintained by a blockchain mechanism by the federation of DMs. Remember that the Layer-2 distributed ledger is different from one in the Layer-1 to keep identification lists. There are several possibilities for the structure of the profile and a wide range of possibilities in realization. Choices are available depending on the service purposes. Without going further into the detail, we simply assume the profile is the history of participants' access information to published articles. The federation shares the information in the distributed ledger so that the points possessed by each participant is fairly treated among several DMs. We will discuss how to reflect accessing the history to the amount of points and how to use the points in the later section of the business model and marketing principles.

F. *Layer 3*

This is the layer where participants publish articles. In the proposed system, the right of publication is managed in a completely distributed manner associated with h-ID. The most important characteristics is that there is no single entity that control the overall communication space so that we can avoid unfair claims of opinions. To ensure the fairness and equal right in publishing articles and comments, there is a boundary in the actions of participants. In the process of publishing, participants consume their point or points upon casting information to the system. The amount of points is managed by the blockchain mechanism so that the chance to express opinions is equally allocated to every participant. The points are calculated based on the charges for reading and rewards for writing, and the actions are reflected to the profiles of the user. Later we will discuss about the how to manage the profile and reflect it to the number of points.

G. *Business Model*

Now, we must consider how to cover the cost of the proposed system. At the beginning, let us review the business models of communication environment in general. Common SNS services are run by a commercial business model meaning that the cost of system performance and maintenance is covered by commercial content sponsors. On the other hand, the publication of research articles is based on the researcher's initial coverage and rewards obtained from the reader would be shared as pay-per-view basis. Online magazines are generally run by a flat charge from readers. Even though we pay for the magazine, system service providers may ask for sponsorship from companies, and readers enjoy information about goods or services as well as articles. So called 'freemium' is a typical practical realization of the service when a large number of people are attracted to it.

The motivation of this article is to consider the possibility of a communication environment in which participants are confident about unbiased content and evaluations. Although, system running costs are unavoidable in any type implementation. We may put aside the issue related to the running cost of the whole system, since the focus of the paper is the feasibility of technical implementations of fairness.

For the rest of discussion in this article, we assume that the total cost of running the whole system should be covered by certain kinds of means that are separated from the activities of the participants. We also assume that there is no differentiation to commercial publications and ordinary articles in the appearance of articles. The reason is the following. Recently there are actions named stealth marketing. It is difficult to categorize one article whether it is a normal publication or a biased marketing article. So, for the sake of discussion, we treat all publications in single flat space. At the same time, we assume the system allocates a limited number of points to a user as in the Layer 3 features. They are consumed upon publishing articles as well as placing any comments on another's articles or evaluating articles. We consider an open source search engine in Layer 3 applications in which the ranking algorithm is disclosed. The proposed example of such point-management and implementation of the search engine will be discussed in the next section.

H. Fair Management of Points

In the proposed environment, each participant is assigned a limited number of points. They are consumed when participants make publications or place a comment on articles. There could be a wide range of possible implementations of such a scheme. In this paper some basic realizations will be discussed in the next section. Here at least one thing must be clearly mentioned, that is about the trustfulness of distributed ledger. Regardless to the scheme adopted for point management, we may be confident about the management of listed data. As far as the operation of DMs is appropriate and faithful to federation rules, the amounts of points are fairly treated by using the blockchain distributed ledger. Here we claim that in the Layer 3 application management of points can be trusted in terms of the assigned numbers whatever counting algorithm is introduced.

IV. Applications over the Layer-3 Communication Environment

So far, we have designed a three-layered structure that in order to ensure anonymous and fair assignment of membership to the community. In this section, we discuss about dynamic operation of individual fairness. Here we will introduce a scheme of points management for participants' actions namely reading and writing articles. Participants donate points upon reading articles to the author of it. When an article is highly applauded by many participants, the author should be appropriately rewarded and that should be associated to the number of points. Here, for the sake of discussion, we consider monolithic point assignment and evaluation of the quality of documents simply by accumulation of the points. Of course, a wide range of sophisticated point management can be considered in relation with money and operation of a web-based service, we put those aspects outside of our focus. In the following, firstly the characteristics of points are explained. Then, one basic assignment procedure of points to the participants will be discussed. In addition to point management, the idea of an open search engine is introduced.

A. Definitions of Points

Points are defined as follows.

① **Participants**: A participant takes part in the communication environment where one can publish articles as well as put comments on another's article. Each action requires consumption of some points.

② **Points assignment**: In every predefined time period, points are equally assigned to every participant, and the points perish according to the time. The length of those generations and disappearances should be well-considered but not discussed in detail in this paper.

③ **Consumption**: In order to take actions such as publication and evaluation of articles, one needs to consume points.

④ **Recommendation**: Articles are evaluated based on the amount of points collected from recommendations by readers. Assigned points to the article do not disappear and are piled up over time. Publications with good reputations could be rewarded with real money but let us put such deals out of scope of this paper. It may need features to avoid multiple recommendations from a single user from a fairness point of view. This could be done without difficulty when the disturbed ledger is properly managed for the points of participants.

⑤ **History of Publication**: We assume that the publication history of a single handle name should be traceable by all other members of the community. The treatment of recommendation history also may be disclosed. There are several possibilities in relation to items in user profiles, whether to disclose or not. It also depends on the implementation.

⑥ **Reputation management**: Evaluation of published articles is primarily done by comments from readers. Ranking of the article is based on the accumulated points. Blockchain data management is applied towards the profile of articles as well as participants' points.

Based on the above-mentioned procedures, published articles are fairly treated by the member of this communication environment. In realization, there are a lot to discuss for the range of implementations. However, what have mentioned are the minimum requirements in the proposed environment.

B. Ranking Service

A general search engine supported by so-called 'platformer' does not disclose its complicated ranking algorithm. From the fairness points of view, it is natural to introduce fair ranking mechanism with an open-source algorithm. For the communication environment under discussion, the range of characteristics of information is limited so that the mechanism could be simple. The platform is managed in a distributed manner which gives the warranty of fairness. It may be healthier when ranking services are implemented by different DMs.

C. Disclosure of Personal Profile

The user profile is handled with a unique handle name which is anonymous. Expressing real-life identity is not necessarily prohibited, it depends on user's choice. In general, the common service providers of SNSs can utilize users' personal history of searching activities for its marketing activities. We cannot resist this situation since this scheme is related to the cost of running the whole system of the provider. In the proposed environment, however, each participant can hide one's own profile by encryption. Each participant cannot change what has been done but need not disclose one's history to others. This is theoretically possible though it requires some implementation and management costs.

D. Incentives and Drawbacks

In this section, the feasibility of the proposed settings is discussed. For the comparison, we start reviewing common SNS environment. The service is run by commercial basis meaning running cost of the system is supported by sponsorship. From the service providers point of view, information circulated inside the system should be appropriate from that aspect. Extreme message needs to be avoided in the communication space. From the participants aspect, a certain amount of commercial information is acceptable and even required. When it comes to the publishing from a participant, there are some concerns such that mentioned at the beginning of this article. From the aspect of constructing healthier communication environment, it is meaningful to manage the whole system with several different DMs, since each DM may work on their own policy of, for example, choosing sponsors. In the Table II, summaries of incentive and drawback of proposed settings.

TABLE II. ENTITY'S INCENTIVE AND DRAWBACK

Entity	Incentive	Drawback
Sponsor	DM may have competition in terms of propagating sponsors information.	Need to negotiate many service providers (DMs) for the sponsorship.
DM manager	New entry to the SNS market, currently dominated by large platforms.	Additional cost to run distributed ledger. Need to collect participants. Less scale merit as a business.
publisher	Confident about balanced criticism from readers.	They may be asked to pay for the publishing depending on DM's policy.
reader	Unbiased reputation to articles and comments.	Switching cost from current service
reviewer (reader)	Confident about faire reputation management	Switching cost from current service

It seems publishers, readers, and commentators do not expect large drawbacks, apart from sophisticated user-interfaces provided by common SNS services. In the implementation of virtual currency with blockchain, they introduce incentive structure that allocate small amount of reward to the miner of correct sequence of the history of distributed ledger. In our proposed settings, DM may carry out innovative mechanisms to maximize their profit independently while participating overall communication environment.

V. INPLEMENTATION WITH WEB SERVICE TECHNOLOGY

So far, we have considered the basic design of an anonymous and fair communication environment. In this section, further discussions about implementation are shown. We introduce a concept of virtualized implementation of the communication environment. To build proposed environment, straight forward implementation is just to construct a web service over a cloud computing environment. One possible implementation is, however, to utilize a Web API of documents which is available when it is published by a common ISP (internet service provider). By using existing services where document publications are possible, the total cost of system implementation could be reduced.

Suppose we have the accounts of the system according to the procedure explained in the above discussed system. There is a communication space where articles are treated only in the form of Web API. The list of the API of documents published by the members. Semantic Web is a technology that uses RDF (Resource Description Framework) as data representation and SPARQL as a query language. The data scheme utilizes a URI (Uniform Resource Identifier) as a node of the data. We can handle whole documents as a set of graphs represented by an RDF format and manage them with a distributed ledger. In Fig. 3, the concept of virtualization is depicted. In the followings, the explanations about this idea are given.

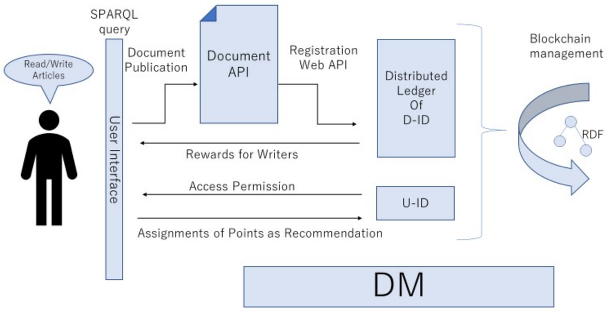

Fig. 3. API managements over DM

A. User Identification

Theoretically we can assume the 3rd-party authenticator that issues anonymous user identification (U-ID) without double counting and disclosing personal data. As explained above, a DM may play a role in this authentication. Once admitted, this URI can store user profile data that is accessible through RESTful Web API [12].

B. *Web API as Document Identification*

When a writer publishes an article on the Internet, the publication may appear either on a common SNS or a personal website. The published article usually has a unique URI. We propose to utilize them as document identifiers (D-IDs) in the distributed ledger. They are managed by a blockchain mechanism with profiles in which writer's handle name and recommendation points are announced. Upon publication from a participant, DM register D-ID associated with U-ID. Those IDs are accessible from both DM and other participants. so that the communication environment could be virtually constructed.

C. *Linked Open Data as the Communication Environment*

Now we adopt the concept of LOD (linked open data) as a software architecture of proposed web service. The scheme has been studied for years [5]. There are several useful data management tools available in the scheme. We may apply some of them for the implementation of the proposed communication environment. As we explained in the previous sections, the necessary information such as U-ID and D-ID, is described in the form RDF and managed by the blockchain platform in the form of a distributed ledger.

D. *Search Engine by SPARQL*

We have proposed to introduce open-source search engine for the participant to be confident about the results of ranking results. As the system handles RDF graph representation, standard SPARQL query applications, such as Sesame, Virtuoso, are available as search engines. They could support sophisticated user interfaces of searching services so that ranking service may not be monopolized by a single provider.

VI. Concluding Remarks

Large scale SNS services give us huge benefits to our daily lives. Consequently, their influence on our public communication became enormous and raises many controversial issues in terms of freedom of speech and protection of privacy. Common SNS services are based on commercial principles. This situation may cause inconvenience in terms of fair treatment of publications.

Recently, blockchain technology has the potential to reform such an environment with its characteristics of a distributed scheme. We proposed a technological realization of a communication environment where participants are not allowed double accounts. This may prevent unfair aggregated criticism to publications. The two-step escrow of identity information make participants confident about their privacy. The proposed protocols are based on the distributed ledger of blockchain and public privacy information escrow. There, anonymity, and fair reputation management can be achieved.

After explaining basic structure, LOD based virtual implementation is shown. This paper only focuses on the aspect of technological feasibilities. We believe that the basic necessary condition is satisfied with the elements discussed in the article. Further discussion may be necessary for real world implementation such as ethical aspect of communication environment.

References

[1] G.Bina Ramamurthy, 'Blockchain in Action', Manning Publications Co., 2019,

[2] S. Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System', http://bitcoin.org/bitcoin.pdf

[3] E. Feig, 'A Framework for Blockchain-based Applications', Mar. 2018, Cornell Univ. Archive, https://arxiv.org/abs/1803.00892

[4] T. Segaran, et. al., 'Programming the Semantic Web', O'Reilly, 2010

[5] D. Wood, et. al., 'Linked Data', Manning, 2014

[6] S. Mullender,edt, 'Distributed Systems', Addison-Wesley,1993, ISBN 0-201-62427-3

[7] Elias Pimendis, Nikolaos Polatidis, "Secure Social Media Spaces for Communities of Vulnerable People", IEEE

[8] Sathya V. et al, "Blockchain Based Cloud Computing Model on EVM Transactions for Secure Voting", Porc. ICCMC 2019

[9] N. Taniguchi, et. al, 'DECIDE: A Scheme for Decentralized Identity Escrow', DIM'05, Nov. 2005, ACM-159593-232-1

[10] Open API tools, https://openapi.tools/

[11] B, Balis,'Hypermedia workflow: a new approach to data-driven scentific workflows, IEEE Proc. 2012 SC Companion: High Performance Computing, Networking Storage and analysis,

[12] A.Fujii, et. al., "Distributed Synchronization over RESTful Web API", Proc. NBiS-2015, 18-th Conf. Network-Based Information Systems