SOTICS 2016

The Sixth International Conference on Social Media Technologies, Communication, and Informatics

ISBN: 978-1-61208-504-3

August 21 - 25, 2016

Rome, Italy

SOTICS 2016 Editors

Andrea Nanetti, School of Art, Design, and Media | Nanyang Technological University, Singapore

Birgit Gersbeck-Schierholz, Leibniz Universität Hannover, Germany

SOTICS 2016

Forward

The Sixth International Conference on Social Media Technologies, Communication, and Informatics (SOTICS 2016), held on August 21 - 25, 2016 in Rome, Italy, was an event on social eco-informatics, bridging different social and informatics concepts by considering digital domains, social metrics, social applications, services, and challenges.

The systems comprising human and information features form a complex mix of social sciences and informatics concepts embraced by the so-called social eco-systems. These are interdisciplinary approaches on social phenomena supported by advanced informatics solutions. It is quit intriguing that the impact on society is little studied despite a few experiments. Recently, also Google was labeled as a company that does not contribute to brain development by instantly showing the response for a query. This is in contrast to the fact that it has been proven that not showing the definitive answer directly facilitates a learning process better. Also, studies show that e-book reading takes more times than reading a printed one. Digital libraries and deep web offer a vast spectrum of information. Large scale digital library and access-free digital libraries, as well as social networks and tools constitute challenges in terms of accessibility, trust, privacy, and user satisfaction. The current questions concern the trade-off, where our actions must focus, and how to increase the accessibility to eSocial resources.

We take here the opportunity to warmly thank all the members of the SOTICS 2016 technical program committee, as well as all of the reviewers. We also kindly thank all the authors who dedicated much of their time and effort to contribute to SOTICS 2016. We truly believe that, thanks to all these efforts, the final conference program consisted of top quality contributions.

We also gratefully thank the members of the SOTICS 2016 organizing committee for their help in handling the logistics and for their work that made this professional meeting a success.

We hope that SOTICS 2016 was a successful international forum for the exchange of ideas and results between academia and industry and to promote further progress in the area of social eco-informatics. We also hope Rome provided a pleasant environment during the conference and everyone saved some time for exploring this beautiful historic city.

SOTICS 2016 Advisory Committee

Petre Dini, Concordia University, Canada & IARIA, USA
Krzysztof Juszczyszyn, Wrocław University of Technology, Poland
Abdulrahman Yarali, Murray State University, USA
Nitin Agarwal, University of Arkansas at Little Rock, USA
Jürgen Pfeffer, Carnegie Mellon University, USA
Andrea Nanetti, School of Art, Design, and Media | Nanyang Technological University, Singapore

SOTICS Special Area Chairs on Social Networks

Feng Gao, Microsoft Corporation, USA
Lynne Hall, University of Sunderland, UK

SOTICS Special Area Chairs on eGovernment

Jennifer Watkins, Los Alamos National Laboratory, USA

SOTICS Special Area Chairs on Media

Claus Atzenbeck, Hof University, Germany / Aalborg University, Denmark

SOTICS Publicity Chairs

Nima Dokoohaki, Swedish Institute of Computer Science (SICS), Sweden
Christine Langeron, Hubert Curien Laboratory, Lyon University, France

SOTICS 2016

Committee

SOTICS Advisory Committee

Petre Dini, Concordia University, Canada & IARIA, USA
Krzysztof Juszczyszyn, Wrocław University of Technology, Poland
Abdulrahman Yarali, Murray State University, USA
Nitin Agarwal, University of Arkansas at Little Rock, USA
Jürgen Pfeffer, Carnegie Mellon University, USA
Andrea Nanetti, School of Art, Design, and Media | Nanyang Technological University, Singapore

SOTICS Special Area Chairs on Social Networks

Feng Gao, Microsoft Corporation, USA
Lynne Hall, University of Sunderland, UK

SOTICS Special Area Chairs on eGovernment

Jennifer Watkins, Los Alamos National Laboratory, USA

SOTICS Special Area Chairs on Media

Claus Atzenbeck, Hof University, Germany / Aalborg University, Denmark

SOTICS Publicity Chairs

Nima Dokoohaki, Swedish Institute of Computer Science (SICS), Sweden
Christine Langeron, Hubert Curien Laboratory, Lyon University, France

SOTICS 2016 Technical Program Committee

Witold Abramowicz, Poznan University of Economics, Poland
Don Adjeroh, West Virginia University, USA
Nitin Agarwal, University of Arkansas at Little Rock, USA
Fernando Albuquerque Costa, Universidade de Lisboa, Portugal
Mehdi Asgarkhani, CPIT – Christchurch, New Zealand
Simon Reay Atkinson, University of Sydney, Australia
Liz Bacon, University of Greenwich, UK
Thierry Badard, Centre for Research in Geomatics - Laval University, Canada
George Barnett, University of California, USA
Grigorios N. Beligiannis, University of Patras, Greece
Lasse Berntzen, University College of Southeast, Norway
Marenglen Biba, University of New York in Tirana, Albania

Copyright Information

For your reference, this is the text governing the copyright release for material published by IARIA.

The copyright release is a transfer of publication rights, which allows IARIA and its partners to drive the dissemination of the published material. This allows IARIA to give articles increased visibility via distribution, inclusion in libraries, and arrangements for submission to indexes.

I, the undersigned, declare that the article is original, and that I represent the authors of this article in the copyright release matters. If this work has been done as work-for-hire, I have obtained all necessary clearances to execute a copyright release. I hereby irrevocably transfer exclusive copyright for this material to IARIA. I give IARIA permission or reproduce the work in any media format such as, but not limited to, print, digital, or electronic. I give IARIA permission to distribute the materials without restriction to any institutions or individuals. I give IARIA permission to submit the work for inclusion in article repositories as IARIA sees fit.

I, the undersigned, declare that to the best of my knowledge, the article is does not contain libelous or otherwise unlawful contents or invading the right of privacy or infringing on a proprietary right.

Following the copyright release, any circulated version of the article must bear the copyright notice and any header and footer information that IARIA applies to the published article.

IARIA grants royalty-free permission to the authors to disseminate the work, under the above provisions, for any academic, commercial, or industrial use. IARIA grants royalty-free permission to any individuals or institutions to make the article available electronically, online, or in print.

IARIA acknowledges that rights to any algorithm, process, procedure, apparatus, or articles of manufacture remain with the authors and their employers.

I, the undersigned, understand that IARIA will not be liable, in contract, tort (including, without limitation, negligence), pre-contract or other representations (other than fraudulent misrepresentations) or otherwise in connection with the publication of my work.

Exception to the above is made for work-for-hire performed while employed by the government. In that case, copyright to the material remains with the said government. The rightful owners (authors and government entity) grant unlimited and unrestricted permission to IARIA, IARIA's contractors, and IARIA's partners to further distribute the work.

Table of Contents

Social TV and "Influencers": Different Users, Different Effects

Angela Fortunato, Roberta Barone, Umberto Panniello, Michele Gorgoglione
Dipartimento di Meccanica, Matematica e Management
Politecnico di Bari
Bari, Italy
e-mail: angela.fortunato@poliba.it

***Abstract*— TV broadcasters are increasingly adopting social TV strategies to affect the viewers' online behavior. The research done so far suggests that different drivers play different roles and their effects are different according to the specific type of online behavior. In order to extend this research, through hierarchical linear regression models, we compare the effects of the different drivers on the online behavior of "influencers", i.e., users having a large number of followers, and "ordinary" users. Despite some limitations, we show relevant differences between the online behaviors of these two kinds of users, particularly the social TV strategies do not affect the online behavior of the "influencers", while some of them affect the online behavior of "ordinary" users.**

Keywords-social TV; engagement; online behavior; influencer.

I. INTRODUCTION

In the context of the "Social TV" phenomenon [2], social networks, as Twitter, have gained a relevant role, by allowing viewers to share online their real-time viewing experiences [1]. On the other hand, broadcasters often use Social TV strategies [2][3][4] to prompt viewers to interact online during the TV programs [3] and then increase the viewers' involvement [5] and the online engagement around the TV programs, that is the amount of viewers' interactions occurring online [3]. Viewers can interact online through different types of behaviors: in particular, on Twitter they can post original tweets, share tweets (retweets), reply to tweets (replies). Previous research found a relationship between some viewers' online behaviors and specific TV programs and contents [13], while few studies have explored the effects of the Social TV strategies on viewers' online engagement. Reference [3] showed that displaying a TV show-related tweet on TV screen increases the number of retweets, while showing a hashtag increases the viewers' online engagement during commercial breaks. Furthermore, reference [9] demonstrated that the effects of Social TV strategies and TV contents on online engagement can be better explained by distinguishing the different kinds of online behaviors (i.e., generating original tweets, sharing tweets and replying to tweets). They found that some strategies positively affect the generation of original tweets and negatively affect retweets and replies, while the absence of a strategy has a negative effect on all kind of behaviors. Moreover, different TV contents have different effects on different kinds of online behaviors. In particular, during commercial breaks the generation of original tweets decreases, while retweets and replies increase.

However, in order to better examine the viewers' online engagement, relevant aspects of online social networks should be considered. In social networks' context, indeed, one of the most relevant aspect characterizing the online behavior is represented by the individual characteristics [10], specifically the influence a user exerts in his/her network to spread information further [10]. This kind of user is called "influencer" [8][10] (also "influential" or "opinion leader" [6]) and generally the behavior is different from the one of the other members of the network, called "ordinary" users [7]. For instance, by analyzing the online behaviors on a Google Groups' sample, reference [11] demonstrated that "influencers" are more likely to post messages and reply to other messages than other members of the network. Therefore, "influencers" are generally characterized by a different behavior in comparison with the remainder of the network. "Influencers" are identified by considering several metrics, such as the number of followers [7][8][10]. The distinction between "influencers" and "ordinary" users is valid also in the Social TV context but no studies have explored their behavior. In particular, no studies explored whether "influencers" and "ordinary" users show different reactions to the TV contents and the Social TV strategies. Therefore, our aim is to examine in depth the effects of Social TV strategies and TV contents on the online behaviors [9], by studying the difference between "influencers" and "ordinary" users.

The paper is structured as follows. The section II depicts the methodology of our research, in terms of dataset, variables' description and method applied to study the relationship between variables. The section III illustrates the preliminary results and conclusions.

II. METHODOLOGY

According to prior research, we want to study the effects of Social TV strategies and TV contents on the online behaviors of "influencers" and "ordinary" users. In order to do so, first we collected approximately 500,000 viewers' tweets during the entire 2015 edition of the Italian TV show "L'Isola dei Famosi", one of the most popular reality show using social TV strategies, where celebrities had to survive on a desert island. During the show (one episode a week for seven weeks), the broadcaster delivered several strategies on the second screen app dedicated to the program. The collected data were further distinguished between original tweets, retweets, replies and tweets generated through the second screen app. Then, we defined two different types of users: "influencers" and "ordinary" users. In order to do so, we measured the number of followers [7][8][10] of each

 ISBN: 978-1-61208-504-3

user and we built a frequency distribution of the number of followers per user. Finally, we identified the group of "influencers" by considering the top 1% of users [12], which are the users with the highest number of followers. The rest of the network has been labeled as "ordinary" users.

In addition, for each minute of the show (including commercial breaks), we measured: the type of TV content shown on screen, the type of Social TV strategy used, the number of viewers, the number of total tweets further distinguished into original tweets, retweets, replies and tweets generated through the second screen app. According to previous research [9], we applied hierarchical multiple linear regressions using the following dependent variables: online engagement (OE), i.e., total number of tweets, and the different kinds of online behaviors, such as original tweets (OT), retweets (RT), replies (RP) and tweets generated through the second screen app (AT). The dependent variables were shifted by a time delay of one minute with respect to the measurement of independent variables [9]. The independent variables are: the TV content, i.e., (1) general contents, (2) challenge, (3) nomination, (4) week summary, (5) contestant's elimination, (6) appearance of eliminated contestant in studio, (7) visit in "Playa Desnuda", (8) start of voting, (9) commercial break; the Social TV strategy, i.e., (1) call to comment, (2) survey/quiz, (3) call to predict, (4) photo gallery, (5) call for appreciation, (6) call to vote, (7) displaying related information, (8) absence of strategy. Finally, we considered viewership and time (the minute within the episode and the number of the episode within the season) as control variables.

III. RESULTS

In this section, we report the main results obtained from our models. For the sake of brevity, we just discuss the statistical significant results (p-value is lower than 0.1) as in [9], without showing any table. We found that viewership positively affects the OE generated by both "influencers" and "ordinary" users. We also found that during the season only the "ordinary" users increase all kinds of online behaviors, while during each episode only the "influencers" increase their online behaviors.

Concerning the Social TV strategies, the results show relevant differences between the two types of users. First of all, the absence of Social TV strategies (strategy 8) has a negative effect on the online behavior of the "ordinary" users, while it does not affect the online behavior of the "influencers". The Social TV strategies do not affect the online behaviors of the "influencers", while some of them, such as strategy (5), negatively affect the online behaviors of the "ordinary" users, and some other Social TV strategies, such as strategy (1), positively affect their posting behavior and negatively affect their sharing behavior.

Looking at the TV contents' effects, we found that some contents (such as content 2 or content 9) generate increases and decreases in different types of online engagement for the two groups of users. In particular, during commercial breaks, i.e., content (9), RT generated by both kinds of users increases. However, "ordinary" users decrease OT and increase both RT and RP, while "influencers" increase only RT. In other words, "influencers" and "ordinary" users react differently to different kinds of TV contents and, in particular, during the commercial breaks, only the "ordinary" users decrease the posting behavior.

In this paper, we have shown the preliminary results of our research, which aims at demonstrating that the distinction between "influencers" and "ordinary" users is useful to explore the effects of Social TV strategies and TV contents in the Social TV context. The results suggest that the two kinds of users are characterized by different behaviors: "influencers" increase the online behaviors during the episode, while "ordinary" users increase the online behaviors during the season. Moreover, "ordinary" users are more affected by Social TV strategies than "influencers", while different TV contents lead to different effects on the online engagement of the two groups of users. As next steps, we will observe in depth the difference between these two kinds of users, by further analyzing the two subsets. In particular, we will include further metrics suggested by the previous literature to identify "influencers" and "ordinary" users, including the "Pareto principle"). Furthermore, we will take into account other similar TV shows in order to confirm these results.

ACKNOWLEDGMENT

We wish to thank Telecom Italia for funding this research, Auditel for allowing the authors to access viewership data, Media Consultants for providing the viewership datasets.

REFERENCES

[1] P. Cesar and D. Geerts, "Past, Present and Future of Social TV: A Categorization," The IEEE Consumer Communications and Networking Conference, pp. 347-351, Jan. 2011, ISBN: 978-1-4244-8789-9

[2] G. Harboe, "In Search of Social Television," in Social Interactive Television: Immersive Shared Experiences and Perspectives, P. Cesar, D. Geerts and K. Chorianopoulos, IGI Global, USA, pp. 1-13, 2009.

[3] S. Hill and A. Benton, "Social TV: Linking TV Content to Buzz and Sales," The International Conference on Information Systems (ICIS), Dec. 2012, pp. .

[4] M. Lochrie and P. Coulton, "Sharing the Viewer Experience through Second Screens," The 10th European Interactive TV Conference (EuroITV), pp. 199-202, July 2012, ISBN: 978-1-4503-1107-6

[5] M. Proulx and S. Shepatin, Social Tv: How Marketers Can Reach and Engage Audiences by Connecting Television to the Web, Social Media, and Mobile. Wiley, 2012.

[6] E. Dubois and D. Gaffney, "The Multiple Facets of Influence. Identifying Political Influentials and Opinion Leaders on Twitter," American Behavioral Scientist, vol. 58, no. 10, pp. 1260-1277, Sept. 2014, doi: 10.1177/0002764214527088

[7] S. Wu, J. M. Hofman, W. A. Mason, and D. J. Watts, "Who Says What to Whom on Twitter," The 20th international conference on World Wide Web, pp. 705-714, Apr. 2011, ISBN: 978-1-4503-0632-4

[8] E. Bakshy, J. M. Hofman, W. A. Mason, and D. J. Watts, "Everyone's an influencer: quantifying influence on twitter," The Fourth ACM International Conference on Web Search

 ISBN: 978-1-61208-504-3

and Data Mining (WSDM), pp. 65-74, Feb. 2011, ISBN: 978-1-4503-0493-1

[9] A. Fortunato, M. Gorgoglione, and U. Panniello, "The Influence of Social TV Strategies and Contents on TV Online Engagement," The Fifth International Conference on Social Media Technologies, Communication, and Informatics, pp. 65-70, Nov. 2015, ISBN: 978-1-61208-443-5

[10] O. Aarts, P. P. van Maanen, T. Ouboter, and J. M. Schraagen, "Online Social Behavior in Twitter: A Literature Review," IEEE 12th International Conference on Data Mining Workshops (ICMW), pp. 739-746, Dec. 2012, ISBN: 978-1-4673-5164-5

[11] D. Huffaker, "Dimensions of Leadership and Social Influence in Online Communities," Human Communication Research, vol. 36, no. 4, pp. 593-617, Sept. 2010, doi: 10.1111/j.1468-2958.2010.01390.x

[12] M. Cha, H. Haddadi, F. Benevenuto, and K. P. Gummad, "Measuring user influence on twitter: The million follower fallacy," The 4th Int'l AAAI Conference on Weblogs and Social Media, pp. 10-17, May 2010.

[13] F. Giglietto and D. Selva, "Second Screen and Participation: A Content Analysis on a Full Season Dataset of Tweets," Journal of Communication, Vol. 64, No. 2, pp. 260-277, Apr. 2014, doi: 10.1111/jcom.120

 ISBN: 978-1-61208-504-3

Facebook as an Interaction Platform in Higher Education:
The Case of an Egyptian Private University

Nourhan Hamdi
Cardiff School of Management
Cardiff Metropolitan University
Western Ave, Cardiff CF5 2YB, United Kingdom
e-mail: nourhamdi@gmail.com

Rasha Abdel Aziz
Business Information Systems Department
Arab Academy for Science & Technology
Miami P.O. Box 1029, Alexandria, Egypt
e-mail: rashaayo@gmail.com

***Abstract*—Current research is continuously examining the benefits of using Social Networking Sites, particularly Facebook, in higher education to enhance the learning process. More specifically, a few researchers have tackled the nature of interaction that takes place on social networks between students and educators, outside the learning and teaching setting. This paper aims to classify and investigate the types of interaction that take place on a closed Facebook group between undergraduate students, faculty members and administration staff in the College of Management at a private university in Egypt. A web application was developed to extract the posts and discussions taking place on the group using the Facebook Graph API. The application then helps in classifying and analyzing the extracted data. Results show that the Facebook group acts as an information-sharing hub for news and announcements, as well as a question and answer platform for academic and non-academic topics involving students, faculty, and college administration staff. The study shows interesting results, such as the appearance of implicit types of interaction due to important features like tagging and liking.**

Keywords- Social Networking Sites; Facebook; Online Interaction; Higher Education; Facebook Groups.

I. INTRODUCTION

The role of social networks is increasingly gaining momentum in today's web-oriented society. Social media can be defined as a group of Internet-based applications built on the ideology and technology of Web 2.0 that allow for the creation and exchange of user-generated content [1]. Social media is known to play an essential role in collaboration, community building, participation and sharing.

One vital aspect of social media is that it uses mobile and web-based technologies to create highly interactive platforms through which individuals and communities can share, discuss, and modify user-generated content [2]. This technology exists in different forms, such as Internet forums, web logs, social blogs, micro blogging, wikis, podcasts, ratings, social bookmarking and social networks [3].

According to Facebook statistics, 1.04 billion users on average were active each day in December 2015; 934 million of them were active daily through their mobile devices [4]. With 22.4 million users as of mid-2014, Egypt is ranked 14th worldwide in terms of audience size, and ranked 1st among Arab countries.

Facebook in Egypt is a youthful community, users younger than 35 years old represent about 85% of total users, while users aged 45 years or older only make up about 5% of total users. Eighteen-year-old users are the largest single-year group on Facebook, with about 1.3 million users, alone representing more than 6% of the total Facebook users in Egypt. The age group ranging from 19 to 24 represents 31% of the Facebook users in Egypt; this is the same age group of the youth studied in this research [5].

Students feel the need to get together, collaborate, have discussions, and exchange information with others who share similar interests [6].

This study analyzes the use of the closed Facebook group created for the Student Union of the College of Management (CMT) and Technology at the Arab Academy for Science and Technology (AAST) [7] in Alexandria, Egypt. The research aims to investigate how Social Networking Sites, in this case Facebook, could be used by the college community in the educational context. This Facebook group was initially created in March 2011 by the college administration to notify students of important general announcements. The admins of the group were all college staff members at that time. Currently, the group admins include both staff members and member students of the CMT Student Union. The admins are responsible for approving the addition of new members and monitoring language and content to make sure it's relevant to the purpose of the group.

The students of CMT are middle/upper class youth, with an age range between 18 and 23. All students must pass an admissions test to prove their English language proficiency, unless they are enrolled in the Arabic department, which comprises 27% of the total number of students enrolled in all departments.

On Facebook, users can perform three actions on each post: like, comment, and share [8]. The group studied in this paper is closed only for members participation and did not allow the option of sharing posts, therefore the data collected only includes the post content, with all its details including number of likes, and the comments that it received.

Previous work that tackled the same area of research are discussed in section 2, followed by the detailed research method and steps in section 3. Section 4 presents and discusses the findings of the research after showing the

 ISBN: 978-1-61208-504-3

analysis results. Finally, in section 5 the conclusion, limitations, and future work are presented and reviewed.

II. PREVIOUS WORK

Many previous studies have focused on exploring the use of social media by as an educational tool [9]. Gafni and Deri have studied the costs and benefits of using social networking in the learning and teaching environment [10].

In a study focused on the Facebook walls of undergraduate students at a UK university [11], Selwyn investigated why and how students communicate on Facebook in relation to their studies. He believes that communication over Social Networking Sites (SNS) corresponds in an electronic way with face-to-face social learning contexts at academic institutions, and further suggests that the conversational and collaborative potential of SNS can be utilized for academic purposes. His study points out how SNS can be used educationally to support communication between students during learning situations, as well as for educator-learner dialogue. SNS provide channels for informal and unstructured forms of learning. On the other hand, Selwyn notes that educators are concerned that social networking may distract learners from their studies.

Selwyn [13] regularly logged in to sites of 909 students, not to participate or interact, but to observe the sites and profiles that were publicly accessible and to systematically archive relevant exchanges. A pattern that emerged was the use of Facebook for practical information, such as schedules and venues. Although this was also available on official channels, some students preferred accessing Facebook for this information. In this paper we decided to explore how SNS can be used to connect a college's community outside the boundaries of a specific course or a specific group. In the case of the group we are studying, the group is considered one of the official college channels of information sharing, as it was created and is moderated by the college administration. Furthermore, Selwyn explored the possibility of merging social and educational environments in order to understand students' purposes for using Facebook and the relationship of their interactions to educational aspects. Five themes emerged from his analysis of over 2000 education-related posts: (1) recounting and reflecting of university experience; (2) exchange of practical information; (3) exchange of academic information; (4) displays of supplication and/or disengagement; and (5) banter (i.e., exchanges of humor and nonsense).

Another study by Pollara [12] explored the use of Facebook to determine if the implementation of social networking in education would strengthen the relationship between mentors and mentees and increase student participation and dialogue outside formal settings. Results indicated that the use of Facebook positively affected the relationships between mentors and mentees. In addition, students believed they learned more by using Facebook and would prefer using it for other educational purposes.

In her study, de Villiers [13] described and discussed a venture in which postgraduate distance-learning students joined an optional group on Facebook for the purpose of discussions on academic, content-related topics, largely initiated by the students themselves. The study revealed that learning and insight were enhanced by these discussions and that the students were benefiting from contact with fellow students.

Most of the studies in the literature have investigated the effect of social networks, especially Facebook, on the learning process and ignored the perspective of exploring what the features and functions, like Facebook groups, could offer to academic institutions and its stakeholders; that is what this paper aims to explore.

III. RESEARCH METHOD

This study analyzes the use of a closed Facebook group created for the Student Union of the College of Management and Technology at the Arab Academy for Science and Technology in Alexandria, Egypt. This Facebook group was initially created in March 2011 by the college administration to notify students of important general announcements.

Using the classification in Mouton's map of research designs [14], the methods used in the study are a combination of content analysis of the posts and quantitative descriptive statistical analysis of the dataset.

A. The Closed Facebook Group

The purpose of using the Facebook group within the college community has evolved over the four years since it was first created. This study analyzes the posts and interactions that happened within the group during the fall semester of the 2015/2016 academic year. Since the Facebook group is a closed group, the researcher was granted administrator permission to have access to content and advanced controls in the group.

a) Group Members

As of January 2016, the number of members in the group had reached 4500 members. This number includes all the faculty, admin staff members, and students that have joined the group since March 2011. Joining the Facebook group is not mandatory, therefore the active number of students is estimated to be a little below the total number of students that are currently enrolled in the College of Management, which is a total of 1701 students.

b) Departments and Courses

The Facebook group is neither course-specific nor department-specific. The members of the group include students from the seven academic departments of the College of Management who are enrolled in the more than 282 courses offered that semester.

B. The Web Application

A web-based application which uses the public Facebook Graph API was developed to retrieve all the posts and comments that took place on the group page starting at the end of September 2015 and ending in

 ISBN: 978-1-61208-504-3

January 2016. The posts were then saved in a database and later analyzed to reach the research findings.

In addition to the post content itself, information like the number of likes, and the name of the user who posted were also extracted from Facebook and stored in the database. To prepare the dataset for analysis, the application helps add descriptive attributes to each post and each comment. The following attributes were used to describe each post:

- Who made the post?
- A classification of the content of the post.
- The language used in the post.
- What was the feedback on the post?

Additionally, special remarks were added to each post to further describe its content and the feedback it received (see Fig. 1).

C. *Ethical Considerations*

Ethical clearance was obtained from the college's research ethics committee before starting the study. A disclaimer was posted on the group to notify all members that the content posted during the semester was subject to academic research. All information and identities were to be kept anonymous and any member was given the right to withdraw his participation and actions from the study.

IV. ANALYSIS AND FINDINGS

A total of 1344 posts and 4580 comments on these posts were collected. After classifying the posts according to content, the role of the user who posted, and the feedback and number of likes, the following analysis were conducted.

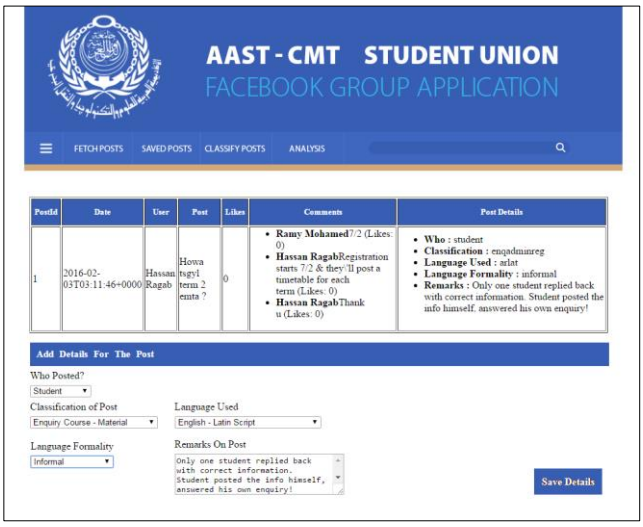

Figure 1. Screenshot of Post Classification Page

A. *Who Posts on the Group*

As shown in Fig. 2, the largest number of users who posted on the group was students and student union members (SU students), with a total of 69% of the collected posts. This was followed by faculty and instructors, representing 22% of the total posts for the semester. The admin staff represented only 7% of the total announcements. Some advertisements were also allowed to be posted on the group by approved training centers and AAST institutes outside CMT.

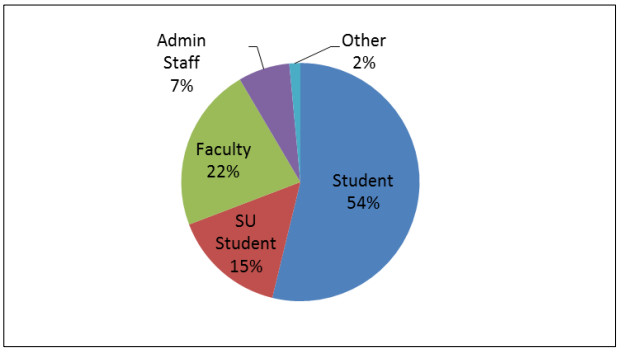

Figure 2. Users Who Posted on the Group

B. *Posts Classification*

After the posts were reviewed, the following classifications were created to describe the content of the posts. The classification process was semi-automated, as it had to include human intervention at some cases. Two major notification types were classified: enquiries and announcements. These two classifications were further grouped into sub-classifications according to the occurrences found in the post content (see Fig. 3 and Fig. 4).

The third frequently used classification was sharing of academic content by students and faculty. Students shared content to help each other before exam times; and some interesting posts were extracted where students took pictures of their handwritten notes and posted them on the group. Faculty also shared course material files like PDFs, PPTs, and video tutorials.

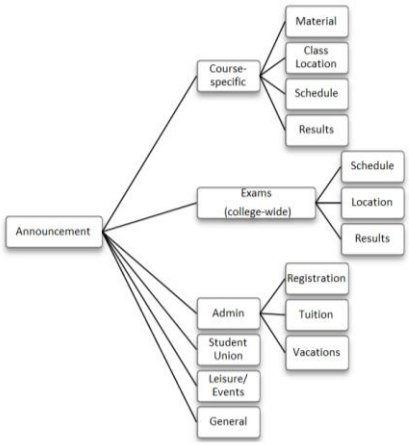

Figure 3. Classification of Posted Announcements

Other types of posts were also identified, such as student complaints, condolences on the occasion of death, and some advertisements posted by entities and other institutes in AAST (e.g., Graduate School of Business, AAST Alumni).

 ISBN: 978-1-61208-504-3

The highest post type used on the group was enquiries (51% of total posts), followed by announcements (36%) see Fig. 5.

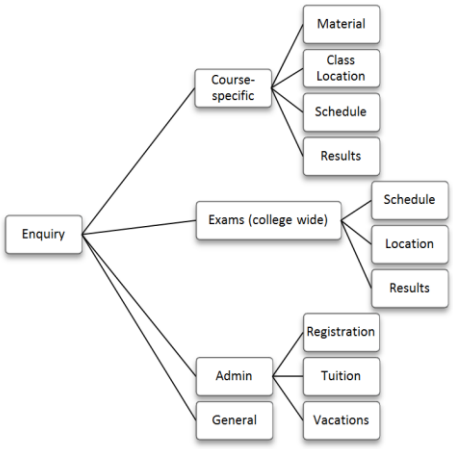

Figure 4. Classification of Posted Enquiries

Students posted 97% of the total enquiries, whereas the announcements were posted by faculty members, student union members and administration staff.

The term "Good Luck" occurred in a total of 37 faculty posts before exam times, to encourage them, and received a high number of likes relative to the average of the total posts by faculty members.

It was detected that the rate of new posts being added to the group increased during specific time periods. After further investigation, Fig. 6 shows how that academic calendar highlights were the reason behind the high rate of posting.

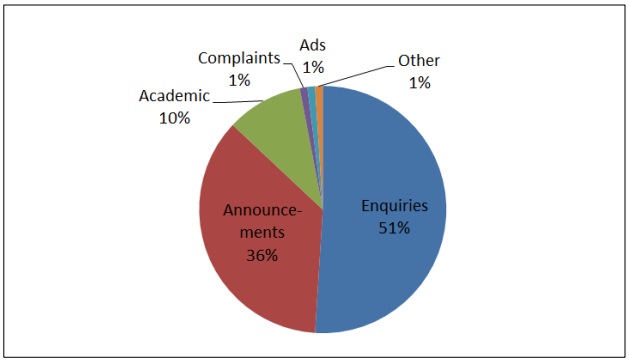

Figure 5. Post Types

Posts were grouped according to the time span of the academic calendar highlights. The highest percentage of post types consisted of enquiries, followed by announcements, and shared academic material during exam times. Example of student enquiries during exam times are asking about exam schedule, chapters included in exams, and asking about grades. Announcements during exam times were made by faculty, Student Union members and admin staff regarding schedules, exam rooms, and course content covered in exams. Furthermore, course material was shared by faculty and students. During registration time, the enquiries were all posted by students to ask about course availability, tuition payment and semester starting dates.

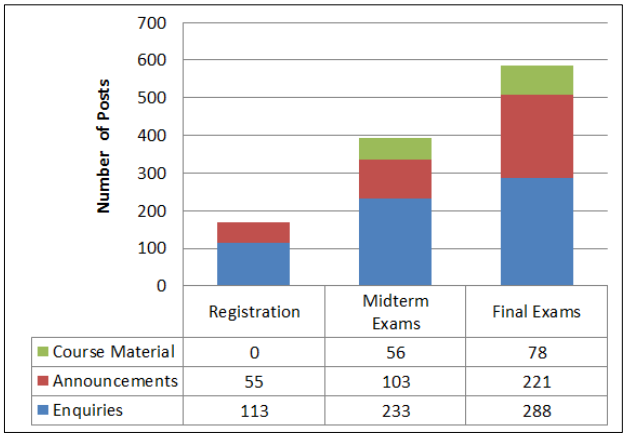

Figure 6. Post Types During Academic Calendar Highlights

C. *Language Used*

Out of the total number of students enrolled in CMT at the time of the study, 99% were native Arabic speakers, which was reflected in the language of the discussions on the group page. The language was classified into English and Arabic, and then further classified according to the script used for writing. The language was classified as shown in Fig. 7.

Fig. *8* shows that the highest number of posts were written in a mix between English and Arabic text written in Latin script; this dual language was used in 92% of the enquiry posts made by students. 31% of the posts were written in English using Latin script, mostly by faculty and SU students in official announcements. 14% of the posts were written in the Latin transliteration of the Arabic language with no English words included.

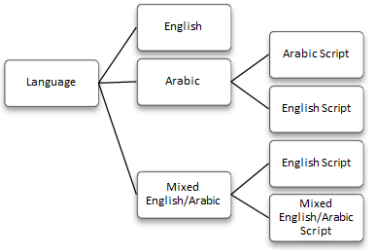

Figure 7. Classification of Language and Script Used

7% of the posts were fully written in Arabic using the Arabic script and were almost all announcements posted by faculty or staff members in the Arabic department of the CMT that were directed to the enrolled students.

 ISBN: 978-1-61208-504-3

D. *Discussions and Feedback on Posts*

A total of 4580 comments was extracted and added to the database to represent the feedback on the posts, along with the number of likes, which could also be extracted using the Facebook API.

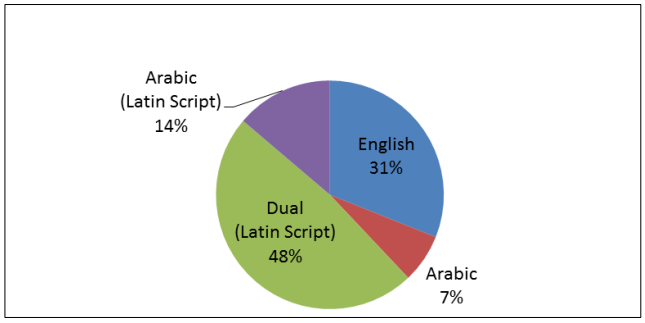

Figure 8. Languages and Scripts Used in Posts

a) Comments

The average number of comments on all the posts in the dataset was 3.4 per post, but not all posts had users comment on them. The posts were classified into seed and non-seed posts [15], the seed posts being those that have developed a thread of comments and discussions, and the non-seed posts being those who have failed to attract engagement from the group members. Posts that received likes but no comments were not counted as seed posts. Interestingly, only 41% of all posts were seed posts, while the rest were non-seed posts. An example of a seed post that gathered a relatively high number of comments is when the campus had to close due to bad weather conditions and the responsible faculty member posted that the following day's classes were cancelled. The post was written in both English and Arabic, and the Arabic language had some humor in it, because the professor who posted knew that students would like taking a day off from college.

Post exclusivity has also been found to have an effect on the post feedback; the post with the highest number of comments was posted by a student who had an exclusive announcement. The same content was posted later three times but did not receive the same amount of feedback.

The comments on enquiry posts were analyzed and classified into positive and neutral feedback. Where positive feedback included helpful information that answers the enquiry and neutral feedback didn't really help with answering the enquiry. Interestingly 83% of the comments on enquiries were positive feedback comments that helped the students by giving them either the solution or answer to their enquiries or helped leading them to it (e.g., tagging friends who had answers).

b) Likes

The like feature on Facebook allows users to press the like button, either on a post or a picture or a comment, which signifies that a user liked that particular content. In the dataset, the average number of likes on posts was 2.5 and the average number of likes on comments was 0.7. The types of posts with the highest average number of likes were announcements, such as exam schedules or exam results. Fig. 9 shows a scatter chart of the number of likes and the number of comments each post in the dataset received. The correlation coefficient r=0.552 which indicates a low positive correlation between the number of likes and the number of comments on each post. The post with the highest number of likes, 239 likes, was a video shared by a student after the graduation projects presentations. The student shot a video including all his friends and all students of the marketing department who were presenting that day. The post received the highest number of likes because everyone could see themselves in the video and the students were proud of their work. The same post received a total of 43 comments, of which 40 comments were students tagging their friends.

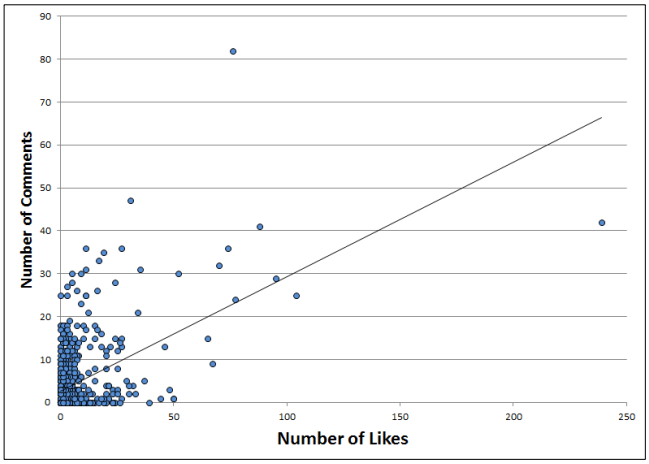

Figure 9. Likes and Comments on Posts

c) Tagging

The tagging feature in Facebook allows users to add the name of another user in a post or a comment, so that the tagged user understands that the posting user wants him involved in that specific topic. Tagging was used in 87% of the comments, where students tagged their friends, or tagged certain faculty members, when they needed them to either answer an enquiry or felt that they needed to notify them with the information being shared in a specific post.

Faculty members explicitly asked the students to tag their classmates in 21 occurrences, when they posted important and urgent announcements. Two posts by students also included a request to tag the teaching assistants, in urgent enquiry posts. On Facebook you can only tag someone who is already on your friend list, hence the need for the tagging request in the posts.

V. CONCLUSION AND DISCUSSION

After analyzing the content of the posts and comments and discussions, as well as all the descriptive data and classification, we concluded that a group on a SNS can act as a variety of interesting platforms for interaction in higher

 ISBN: 978-1-61208-504-3

education institutions. A study by Mbodila et al. [16] on the effect of social media on students engagement recommended that in order to communicate effectively with students, higher education professionals must embrace new technologies and explore opportunities to implement a social media presence; this is what was taking place on the CMT closed Facebook group. The interaction between the members of the group allows us to conclude that SNS can help the higher education communities, outside interact by acting as a (1) notification center; (2) question and answer platform; (3) student affairs portal; (4) learning management system.

A. *Notification Center*

The group acted as a notification center where announcements were made about all activities that can happen on a college campus. It was used for information sharing between students, as well as between students and faculty and college admin staff.

B. *Question and Answer Platform*

The group acted as a question and answer platform where students could enquire about anything related to their studies, courses and exams. They were either answered by other students or by faculty and staff members. This created engaging collaboration between students, outside the boundary of a specific course or educational setting.

C. *Student Affairs Portal*

The student affairs administration staff used the group to share information and announcements; students also used it for their student affairs-related enquiries.

D. *Learning Management System*

10% of the total collected posts were shared academic content of different courses, either by students or by faculty members. Moodle [17] is being used by CMT as a learning management system since 2009 for all courses in course material sharing, assigning submissions etc. Despite this fact, it was interesting to observe that both faculty and students also used the Facebook group as a mean of material sharing.

E. *Implicit Interaction*

Interesting implicit interaction was detected when students used the Facebook tagging feature to tag their friends on important notification posts. After seeing the tag, the friends often liked the comment that included the tag, as confirmation that they were aware of the announcement of the post. This was possible due to the tag and like features provided by the Facebook, and occurred in 81% of the total posts announced by faculty and staff members.

Although the frequency of their appearance was relatively low, emojis [18] found in posts and comments did sometimes hide implicit meanings like sarcastic smiles, or conveying a message without actually typing it in text. The use of emojis could be further investigated in future work.

F. *Limitations*

It is inevitable that interaction on the group continues after the dataset was collected, more likes and comments are added by the users. This results in extended discussions that could not be included in the dataset because they did not exist at data collection time. In March 2013, Facebook announced a new feature [19] that enables the users to directly reply to specific comments left on any post instead of generally replying to the post. This feature makes it easy to keep relevant conversations connected, but when the comments in our study were collected, there was not differentiation between comments on a specific post, and comments replied to a specific comment on that post. All comments were treated equally in our study.

A further limitation that hindered the study from having more elaborate statistical results of the students interacting on the group, is that the total number of students enrolled in the Facebook group includes students that have already graduated. Furthermore, not all the students registered at the college during the semester have Facebook accounts or are members of the group.

G. *Future Work*

As a result of the study, we observed that some important posts were not found interesting and were neglected by students. As future work, the reasons behind this could be explored and we could help recommend how to create more interesting content for students with which they will be willing to interact.

This paper is not intended to prove that Facebook is better than learning management systems that are originally designed for educational purposes, but a comparison between the two could be further explored in future investigations.

Furthermore, the degree of formality of the used language and the sentiments detected from the comments were also observed and could be explored in future work.

ACKNOWLEDGMENTS

Our thanks goes to the administration of the College of Management at AAST for granting us access and admin permissions to the college's closed Facebook group to conduct our research.

REFERENCES

[1] A. M. Kaplan and M. Haenlein, "Users of the world, unite! The challenges and opportunities of Social Media," Bus. Horiz., vol. 53, no. 1, pp. 59–68, 2010.

[2] J. H. Kietzmann, K. Hermkens, I. P. McCarthy, and B. S. Silvestre, "Social media? Get serious! Understanding the functional building blocks of social media," Bus. Horiz., vol. 54, no. 3, pp. 241–251, May 2011.

[3] J. P. Mazer, R. E. Murphy, and C. J. Simonds, "I'll See You on," Commun. Educ., vol. 56, no. 1, pp. 1–17, Dec. 2006.

[4] Facebook Newsroom, "Facebook Statistics," 2016. [Online]. Available: http://newsroom.fb.com/company-info/. [Accessed: 10-Aug-2016].

[5] E-Marketing Egypt, "Facebook In Egypt - Online Competitive Intelligence Report," 2014.

 ISBN: 978-1-61208-504-3

[6] N. Eteokleous, D. Ktoridou, I. Stavrides, and M. Michaelidis, "Facebook -a Social Networking Tool for Educational Purposes: Developing Special Interest Groups," ICICTE Proc., no. 2008, pp. 363–375, 2012.

[7] "AAST Website." [Online]. Available: http://www.aast.edu/en/. [Accessed: 10-Aug-2016].

[8] K. Taylor and O. Alonso, "Insights From Brands in Facebook," Proc. 2014 ACM Conf. Web Sci., 2014.

[9] F. Tiryakioglu, "Use of Social Networks as an Education Tool," Contmporary Ecucational Technol., vol. 2, no. 2, pp. 135–150, 2011.

[10] R. Gafni and M. Deri, "Costs and benefits of Facebook for undergraduate students," Interdiscip. J. Information, Knowledge, Manag., vol. 7, pp. 45–61, 2012.

[11] N. Selwyn, "Faceworking: exploring students' education related use of Facebook," Learn. Media Technol., vol. 34, no. 2, pp. 157–174, 2009.

[12] P. Pollara and J. Zhu, "Social Networking and Education: Using Facebook as an edusocial space," Proc. Soc. Inf. Technol. Teach. Educ. Int. 2011, pp. 3330–3338, 2011.

[13] M. R. R. De Villiers, "Academic Use of a Group on Facebook : Initial Findings and Perceptions Literature Study General Use by University Students," Informing Sci. IT Educ. Conf., pp. 173–190, 2010.

[14] "Mouton, J. (2001) How to Succeed in Your Master's and Doctoral Studies: A South African Guide and Resource Book. Van Schaik, Pretoria. - Open Access Library." [Online]. Available: http://www.oalib.com/references/15496255. [Accessed: 24-Jan-2016].

[15] M. Rowe and H. Alani, "Mining and comparing engagement dynamics across multiple social media platforms," Proc. 2014 ACM Conf. Web Sci. - WebSci '14, pp. 229–238, 2014.

[16] M. Mbodila, B. Isong, and K. Muhandji, "The Effect of Social Media on Student ' s Engagement and Collaboration : a case study of University of Venda using Facebook," J Commun., vol. 5, no. 2, pp. 115–125, 2014.

[17] L. Deng and N. J. Tavares, "From Moodle to Facebook: Exploring students' motivation and experiences in online communities," Comput. Educ., vol. 68, no. January 2016, pp. 167–176, 2013.

[18] L. Stark and K. Crawford, "The Conservatism of Emoji: Work, Affect, and Communication," Soc. Media + Soc., vol. 1, no. 2, p. 2056305115604853, 2015.

[19] "Facebook comment replies feature." [Online]. Available: https://www.facebook.com/notes/journalists-on-facebook/improving-conversations-on-facebook-with-replies/578890718789613/. [Accessed: 10-Aug-2016].

 ISBN: 978-1-61208-504-3

Learning Support Method of Information Ethic by a Virtual Network Isolating Risky Messages to SNS

Hajime Iwata , Kento Inoue
Kanagawa Institute of Technology
Department of Information Network and Communication
Atsugi, Japan
e-mail: hajimei@nw.kanagawa-it.ac.jp, inoue@nwlab.org

***Abstract*—Social networking services (SNSs), which are global phenomena, allow users to share messages with others, resulting in a rapid widespread distribution. Because an inappropriate post may cause trouble for a user, it is important for a user to be aware of potential issues. In this study, we propose an information ethics system to determine the degree of risk of a post. When the system detects a high-risk post, it isolates the post on a virtual network.**

Keywords- SNS; Social Networking Service; Information Ethics; Virtual Network; OpenFlow .

I. INTRODUCTION

The Internet is ubiquitous, and many users enjoy social networking services (SNSs), which promote communications with others around the globe. On a SNS network, a user posts a message willingly and other users provide feedback in a short timeframe, allowing a user to receive approval from others. Occasionally a user receives negative feedback when sharing an inappropriate post, image, or video. Often inappropriate content spreads quickly before the user can retract the post. Thus, a user must always be aware of whether a post contains problematic content. However, users, especially those unfamiliar with SNSs, have a low consciousness of a post's risk.

In this study, we suggest a system that can learn information ethics by checking the degree of risk of a user's posts. The user posts on a SNS via a virtual network. The virtual network evaluates the risk of the post. Typically, the virtual network posts directly to the SNS. However, if the system detects a high-risk post, it isolates the post on a virtual network and sends a warning to the user, allowing the user to naturally learn about information ethics.

Section 2 describes the feature of our study. Section 3 describes the architecture of the proposed virtual network system. Finally, section 4 concludes this paper.

II. FEATURE OF OUR STUDY

Twitter is one example of a SNS with many users. In Twitter, the privacy settings are public and protected. When other users see a post, they can easily share a public post via the retweet function. Furthermore, many users post messages that unconsciously include personal information, which others can easily extract. Through this process, posts, including inappropriate ones or those with sensitive information, spread in a short time. In addition, the likelihood that emotional contents are included is high because Twitter users post in short sentences. Herein we suggest an information ethics learning support system for Twitter users.

We established a risk analysis system server on a virtual network. This system transmits a user's post once to a virtual network. If the content is problematic, this system stops the post from going public, reducing fears of inappropriate posts from being scattered on the Internet. This system also issues a warning to the user that a post is inappropriate by transmitting a message to the user from the virtual network. In addition, posts with privacy breaches of the users are stored in the virtual network. Because such posts are handled in a virtual network, the contents are not watched by a third party nor are they rapidly spread on the Internet.

III. SYSTEM SUMMARY

Fig. 1 overviews the constitution of the network. The virtual network increases the flexibility of the overall constitution and the placement of the system by controlling it using OpenFlow [1]. For OpenFlow controller, we set a packet of SNS client software installed in a client PC. The OpenFlow switch can divide a posting packet to SNS in two from a packet transmitted from a client PC.

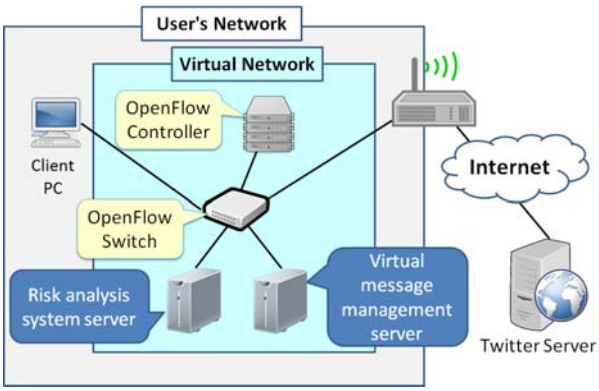

Figure 1. Constitution of the network

 ISBN: 978-1-61208-504-3

This system is easy to install in existing networks. Because this system is implemented using JAVA, it is independent of the platform. In addition, we intended for Twitter by this system as SNS. The access to Twitter uses Twitter4j [2] as a library and free (no cost) open use is possible.

Fig. 2 shows the structure of the risk analysis system. The system initially reads the new post of the user and evaluates it based on the user's previous Twitter posts. Then the system conducts a morphological analysis for a message. Currently, the system only supports posts written in English or Japanese. The English morphological analysis uses Stanford Log-linear Part-Of-Speech Tagger [3], while the Japanese morphological analysis uses lucene-gosen [4].

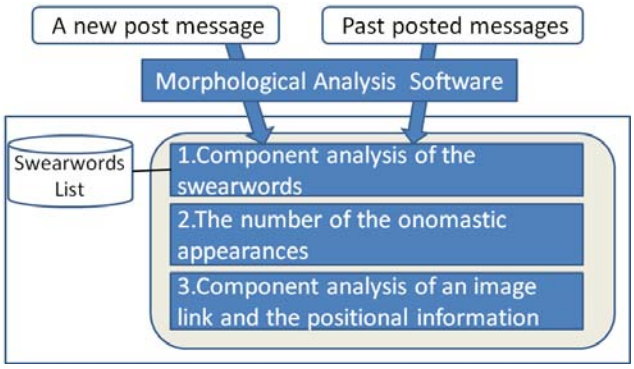

Figure 2. Structure of the risk analysis system

A morphological analysis library allows the system to evaluate the words in a post. This system is based on three factors:

1. Component analysis of the swearwords

The risk analysis system reads a list of swearwords stored on the server. This system compares each word in the message to the list of swearwords and analyzes the risk based on the number of swearwords. Currently, the list of swearwords is compiled manually. The swearwords include profanity, inflammatory, discriminative, and crime-related terms. In addition, the swearwords are converted into a basic form after the morphological analysis and a conjugation before converting to a list.

2. Number of the onomastic appearances

The risk analysis system stores proper nouns, including names and locations. Proper nouns in a message are not immediately considered risky. However, a proper noun becomes an identifiable factor when it appears consecutively in a short timeframe. When the number of the onomastic appearances continues, this system warns the user. Thus, this system can highlight risks to the user.

3. Component analysis of an image link and the positional information

When a link to an image is included in a post, the risk analysis system warns the user. Because automatically analyzing the content of image data is difficult, the system confirms that inappropriate contents are not included. In addition, this system determines whether a post contains GPS information because such information increases the risk that personal information such as the user's home address can be identified. When positional information is included in a post, this system provides a warning to the user.

If a message is problem-free according the risk analysis system, the virtual server posts the message to Twitter. When an item is risky, the virtual server sends a warning to the user and does not post the message to the actual Twitter server. This system encourages users to correct the content. Because the contents of the messages accumulate on the server in a virtual network, the user can ignore the warning. However, the message is not transmitted outside the virtual network, preventing public comments and retweets on a public server. However, the server on the virtual network allows replies and retweets from virtual users, and the system displays issues with the message. Thus, the user can experience the consequence of an inappropriate post virtually, allowing the user to learn information ethics on a non-public server.

IV. CONCLUSION

In this paper, we propose a system that learns and then teaches users about information ethics of SNSs. Our system teaches users about risky situations and the consequences of an inappropriate message on a virtual system, which is more effective than a user learning on a public SNS.
Future works include:

- Implementation of the server on a large-scale virtual whole network
- Automation of the system populating the swearwords list
- Improvement of the examples of trouble from a risky message

REFERENCES

[1] N. McKeown, et al., "OpenFlow: enabling innovation in campus networks", ACM SIGCOMM Computer Communication Review,38, 2 (March 2008), pp.69-74, 2008.

[2] "Twitter4J - A Java library for the Twitter API", http://twitter4j.org/en/ (July, 2016)

[3] The Stanford Natural Language Processing Group, "Stanford Log-linear Part-Of-Speech Tagger", http://nlp.stanford.edu/software/tagger.shtml, (July, 2016)

[4] "lucene-gosen", https://github.com/lucene-gosen/lucene-gosen, (July, 2016)

 ISBN: 978-1-61208-504-3

Discovering Overlapping Community Structure in Social Networks

Z. Bahrami Bidoni
Department of Computer and Information Systems
Clark Atlanta University, Atlanta, GA, USA
Email: z.bahrami@students.cau.edu

Khalil Shujaee
Department of Computer and Information Systems
Clark Atlanta University, Atlanta, GA, USA
Email: kshujaee@cau.edu

Roy George
Department of Computer and Information Systems
Clark Atlanta University, Atlanta, GA, USA
Email: rgeorge@cau.edu

***Abstract*—The massive growth of social networks has created a need for the development of algorithms and systems that can be used for their analysis. Techniques that reveal the structure and the information flow within the network can be used to understand the dynamics of the network and provide new opportunities in promoting virtual communities for a variety of purposes. The basis of this research work is the understanding of a social network community, with special emphasis on communities that overlap. A community is defined as a subgraph with a higher internal density and a lower crossing density with others subgraphs. In this research, we apply a distance based ranking algorithm, the Overlapped Correlation Density based Partitioning (OCDP), to understand communities that overlap. We introduce the OCDP algorithm, and present preliminary results of the technique through its application to a real world data set, the Bottlenose dolphin network. The OCDP is compared with other algorithmic approaches, and in preliminary results show that it has good performance across different evaluation metrics.**

Keywords: ***Dynamic social network, Organizational structure, Overlapping Community discovery, Correlation Density Rank***

I. INTRODUCTION *(HEADING 1)*

Community detection is an significant issue in social network analysis, where the objective is to recognize related sets of members such that intra-community associations are denser than inter-communities associations [2][3][5][6][8]-[11][14][15]. Researchers have presented various methods to extract communities from an SN that paper [17] presented a survey of these studies. Specifically, discovering the organizational structure of communities in an SN has been identified as an interesting but challenging problem [4,13]. Examples of important applications include characterizing potential key candidates for viral marketing or discovering core members of criminal group in monitoring criminal network [13]. Research on finding motivated members in a Social Networks is one component of this researhc, but outcomes have limited power to supply a complete view of the organizational structure.

In the real-world networks, communities are often not disjoint but overlapped to some extent [19]. For example, in social life, a person usually has connections with several social groups such as family, friends, and colleagues; a researcher may collaborate with other researchers in different fields. This can also happen in many other complex networks including biological networks, online social networks, and so on. Indeed, overlap is quite a significant feature in real-world social networks [20]. For this reason, researchers have paid attention to the problem of overlapping community detection, and many techniques have been proposed, such as the the Link method which reinvents communities as groups of links rather than nodes [21], fuzzy c-means clustering [22], and the algorithms utilizing local expansion and optimization including LFM (Local Fitness Maximization) [23], UEOC (the Unfold and Extract Overlapping Communities) [24], DenShrink (Density-based Shrinkage) [25] and the method based on a local definition of community strength [25]. A review of overlapping community detection algorithms is found in [26] along with quality measures and several existing benchmarks. The authors have previously defined the Community Density Rank [18], a measure that is used to evaluate the structure of a community. In this research paper, we extend the CDR algorithm to define the Overlapped Correlation Density based Partitioning (OCDP), to understand communities that overlap, and present initial results from the application of the algorithm to a real world data set, the Bottlenose dolphin network. The OCDP is compared with other algorithmic approaches, and it is shown that it has an equal performance with several published algorithms over a publicly available community data set, the Bottlenose Dolphin Network. It should be noted that this research effort is a work in progress, and though promising the OCDP has to be validated over much larger data sets.

The rest of the paper is organized as follows. Section II introduces the methodology and outlines the OCDP. Section III presents the results of the analysis on a real life data set and Section IV concludes the paper and proposes future work.

II. METHODOLOGY

In the analysis of a network, the first task is to compare nodes. In order to execute this task, the importance of each node within the network has to be understood. The nodes

 ISBN: 978-1-61208-504-3

that link to many other important nodes are themselves important. This process of analysis is similar to PageRank based algorithms [24]. The PageRank algorithm is the best known of these approaches, having been the basis of the original search mechanism for Google. Here the global "importance" ranking for every web page is obtained by analyzing links among web pages. Other algorithms that improve on PageRank such as HITS, OPIC and etc. have been proposed.

The OCDP computation proceeds in two parts- first we compute the Correlation Density Rank (CDR) of each node, and second, we use the CDR to find core nodes and the nodes associated with the cores (the community). The Correlation Density Rank (CDR), is based on finding more frequent and influential Randomized Shortest Paths(RSP)[57] between nodes. In RSP model, the randomness of the walker is constrained by fixing the relative entropy between the distribution over paths according to the reference probabilities and the distribution over paths that the walker actually chooses from. With this constraint, the walker then chooses the path from the probability distribution that minimizes the expected cost. We employ the RSP measurement method in [23] as the distance between nodes, but with one major difference: we consider customized initial cost for edges such that, along with finding shortest path between nodes. The random walker intelligently selects the most important neighbor resulting in lower cost and smaller distance. The CDR considers the distance between nodes as punishment and computes the density ranks of nodes. Hence, there will be a larger traffic amongst shortest path of nodes, if the distance becomes smaller. If the distance between nodes, *i* and *j* was less than the distance between *i* and *k*, then, *i*'s rank effect on *j* is more than on *k*, and the probability that a random surfer reaches *j* from *i* is more than the probability to reach *k*. Therefore, the objective is to minimize punishment so that a node with less distance entropy to have a higher rank. The CDR scores of a node are compared with the nodes in its vertex border to determine the "core" of the community. Communities are then constructed around the cores iteratively, using a membership formulation, where each node can participate with communities formed by multiple cores.

Definition 1 (Cardinality of a community). The cardinality of a community C is the number of its vertices. It is denoted by $|C|$.

Definition 2 (Direct neighbor). In the graph *G = (V, E)*, the vertex v is a direct neighbor of the node u if v and u are connected by an edge. This relationship is represented by the edge $(v,u) \in E$.

Definition 3 (Vertex border). It is all the direct neighbors of node v in the graph. This set is noted by B(v). More formally this quantity is noted as follows:

$$B(v) = \{u \in V;\ \ \{u,v\} \in E\}$$

Definition 4 (Internal Degree of a vertex to a community). We call internal degree of a vertex v to a community C as the number of edges that point towards members of C**.**

$$d_{in}(v,C) = \left|\{(v,v') \in E,\ \ v' \in C\}\right|$$

Definition 5 (External Degree of a vertex to a community). We call external degree of a node v to a community C as the number of its direct neighbors who are not in C**.**

$$d_{ext}(v,C) = \left|\{(v,v') \in E,\ \ v' \notin C\}\right|$$

Definition 6 (Average distance between a node and a community). It is the sum of distances of node u to different nodes $v \in C$, divided by the cardinality of C**.**

$$dist_{avrage}(u,C) = \begin{cases} \dfrac{\sum_{v \in C} RSP(u,v)}{|C-1|} & if\ \ u \in C \\ \dfrac{\sum_{v \in C} RSP(u,v)}{|C|} & otherwise \end{cases}$$

Definition 7 (Weighting coefficient). It is the degree of compactness of one node u to a community C**.**

$$\rho(u,C) = \frac{|B(u)|}{d_{in}(u,C)}$$

Definition 8 (Membership degree). The membership degree of node v to community C is given by:

$$Md(u,C) = \frac{1}{dist_{avrage}(u,C) * \rho(u,C)}$$

Definition 9 (Influence Cofficient degree) where λ is the parameter of control overlapping extent of communities.

$$F_C^u = 2\frac{\lambda * dist_{in}^u - (1-\lambda) * dist_{ext}^u}{dist_{in}^u + dist_{ext}^u}$$

Algorithm 1. Calculating m-Score for members: Correlation Density Rank (CDR)

Input: social network G

Out: vector of m-Score for all members R

1. Initialize cost distance matrix C
$$C[i,j] = \log^{(1-\exp(-\gamma f_{ij}))}_{(1-w_{ij}^{in} w_{ij}^{out})}$$
2. Finding the matrix of RSP dissimilarities [43]:
{
   a. $W \leftarrow P^{ref} \circ \exp(-\beta C)$

b. $Z \leftarrow (I - W)^{-1}$

(Note that $(I - W)^{-1} \approx I + W + W^2 + W^3 + \ldots$)

c. $S \leftarrow \left(Z\left(C \circ W\right)Z\right) \div (Z + \varepsilon)$

d. $\tilde{C} \leftarrow S - ed_s^T$

e. $\Delta^{RSP} \leftarrow \lambda\tilde{C} + (1-\lambda)\tilde{C}^T \qquad 0 \le \lambda \le 1$

}

3. M ← Normalize matrix Δ^{RSP} on rows
4. For each node n_i ($1 \le i \le k$) compute the entropy of related row from matrix M:

a. $E_i \leftarrow -\frac{1}{Lnk}\sum_{j=1}^{k} M_{ij} Ln(M_{ij})$

b. $d_i \leftarrow 1 - E_i$

c. $R_i \leftarrow d_i \Big/ \sum_{i=1}^{k} d_i$

5. Return R

Algorithm 2: Overlapped Correlation Density based Partitioning (OCDP)

Data: A graph $G = (V, E)$

Begin

1: Calculate Correlation Density Rank of all nodes (see Algorithm 1)

2: *u*, if *CDR(u)* > *CDR(B(u))* → *u* is core of the Community

3: For all cores do extend algorithm {

Build border of C: $edg(C) = \{v_i \mid v_i \in B(C)\}$.

While ($edg(C) \neq \varnothing$) do

Choose the candidate node v_i of $edg(C)$ which has the highest membership degree to C.

If $F_C^{v_i} > 0$ *then*

$C \leftarrow \{C\} \cup \{v_i\}$

Update of $edg(C)$

else

$edg(C) \leftarrow \varnothing$

end

End

Return C

End.

III. RESULTS

An experimental analysis of OCDP using a publicly available data set is described. We compared OCDP with five well-known algorithms: (1) CFinder (CPM) which implements the clique percolation (2011); (2) COPRA which is based on label propagation (2010); (3) GCE greedy approach (2013); and (4) EAGLE modularity-based approach (Eagle Community Detection Algorithm, 2012). (5) DOCNet (2014). Bottlenose dolphin network is the real and well-known Dolphins social network which describes the associations between 62 dolphins living in Doubtful Sound, New Zealand (Figure 1). The relationship between dolphins represent the statistically significant frequent association between them. This network is interesting because, during the course of the study, the dolphin group split into three smaller subgroups following the departure of key members of the population. In four commonly used measures in the overlapping community structure research, the modularity, Q_{ov} ; the M rank; number of detected overlapping nod es O_n^d and detected memberships O_m^d,) the OCDP had similar or better results (Table 1). The measure evaluations are as follows (indicates better performance): Q_{ov}, O_n^d, O_m^d: higher, M: lower. While the results of the OCDP in comparison to other published techniques looks promising, it should be noted that this is a research effort in progress.

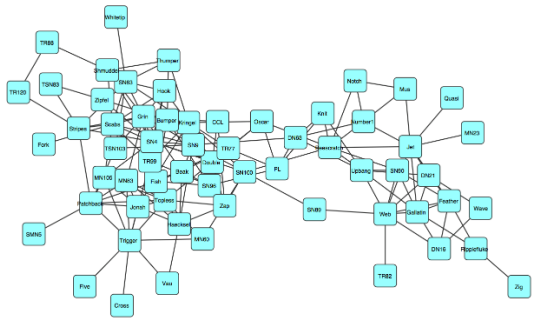

Figure 1. Bottlenose dolphin network.

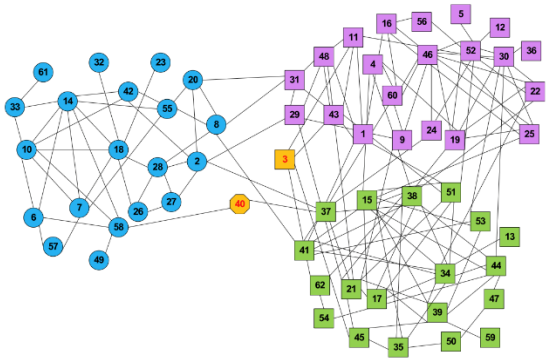

Figure 2. Detected overlapped Communities in Dolphin Network

TABLE I. QUALITY MEASURE COMPARISON

	COPRA (2010)	CPM (2011)	EAGLE (2012)	GCE (2013)	DOC-NET (2014)	OCDP (2015)
Q_{ov}	0.32	0.29	0.32	0.33	0.41	0.47
M	3.00	4.00	4.00	4.00	3.00	3.00
O_m^d	2.00	2.00	2.00	2.00	2.00	2.00
O_n^d	1.75	2.00	1.50	2.00	1.66	2.00

IV. CONCLUSION

Social networks have become an ubiquitous feature of a highly connected global network of users. Analysis of these networks is difficult due to the massive scale of the network and the complexity of the connectivity. Of special interest is the structure and the information flow within the network. Knowledge of these may be leveraged to provide a basis for virtual communities that interact to achieve common goals in a number of domains. In this research, we developed an algorithm the Overlapped Correlation Density based Partitioning (OCDP), that attempts to understand the structure of communities that share members. We present preliminary results of the OCDP technique through its application to a real world data set, the Bottlenose dolphin network. The Dolphin network while interesting is somewhat limited in the number of participants and their interactions. Currently popular social networks involve hundreds of millions of participants, with billions of interactions and the scale up of this technique needs to be investigated.

ACKNOWLEDGMENT

This research is funded in part by the Department of Energy under Contract Number DE-NA 0002686. Any opinions, findings, conclusions or recommendations expressed here are those of the author(s) and do not necessarily reflect the views of the sponsor.

REFERENCES

[1] Kathleen M. Carley, Jana Diesner, Jeffrey Reminga, Maksim Tsvetovat, "Toward an interoperable dynamic network analysis toolkit, Decision Support Systems," 43 (2007) 1324–1347. 1

[2] C. Chekuri, A. Goldberg, D. Karger, M. Levin, C. Stein, "Experimental study of minimum cut algorithms," The Proceedings of the 8th SAIM Symposium on Discreet Algorithm, 1997, pp. 324–333. 2

[3] C. Ding, X. He, H. Zha, M. Gu, H. Simon, "A min–max cut algorithm for graph partitioning and data clustering," The Proceedings of the 2001 IEEE International Conference on Data Mining, 2001, pp. 107–114. 3

[4] Amit Goyal, Francesco Bonchi, Laks V.S. Lakshmanan, "Discovering leaders from community actions," The Proceedings of 17th ACM conference on Information and knowledge management, 2008, pp. 499–508. 4

[5] L. Hagen, A.B. Kahng, "New spectral methods for ratio cut partitioning and clustering," IEEE Transactions on Computed Aided Design 11 (9) (1992) 1074–1085. 6

[6] Bo Long, Xiaoyun Wu, Zhongfei (Mark) Zhang, "Community learning by graph approximation," The proceedings of 7th IEEE International Conference on Data Mining, 2007, pp. 232–241. 7

[7] Hao Ma, Haixuan Yang, Michael R. Lyu, Irwin King, "Mining social networks using heat diffusion processes for marketing candidates selection," The proceedings of 17th ACM conference on Information and knowledge management, 2008, pp. 233–242.8

[8] M.E.J. Newman, "Fast algorithm for detecting community structure in networks," Physical Review E 69 (2004) 066133.9

[9] M.E.J. Newman, M. Girvan, "Finding and evaluating community structure in networks," Physical Review E 69 (2) (2004) 1–15.10

[10] J. Shi, J. Malik, "Normalized cuts and image segmentation," IEEE Transactions on Pattern Analysis and Machine Intelligence 22 (8) (2000) 888–905.11

[11] Andrew Y. Wu, et al., "Mining scale-free networks using geodesic clustering," The Proceedings of 10th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2004, pp. 719–724. 12

[12] Jennifer J. Xu, Hsinchun Chen, "Fighting organized crimes: using shortest-path algorithms to identify associations in criminal networks," Decision Support Systems 38 (2004) 473–487.13

[13] J. Jennifer Xu, Hsinchun Chen, "CrimeNet explorer: a framework for criminal network knowledge discovery," ACM Transactions on Information Systems 23 (2) (2005) 201–226.14

[14] Xiaowei Xu, Nurcan Yuruk, Zhidan Feng, Thomas A.J. Schweiger, "SCAN: a structural clustering algorithm for networks," The Proceedings of the 13th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2007, pp. 824–833.15

[15] Ding Zhou, Eren Manavoglu1, Jia Li, C. Lee Giles, Zha Hongyuan, "Probabilistic models for discovering e-communities," The Proceedings of the 15th international conference on World Wide Web, 2006, pp. 173–182.16

[16] Kivimäki, Ilkka, Masashi Shimbo, and Marco Saerens. "Developments in the theory of randomized shortest paths with a comparison of graph node distances." Physica A: Statistical Mechanics and its Applications 393 (2014): 600-616.17

[17] Malliaros, F. D., & Vazirgiannis, M. (2013). "Clustering and community detection in directed networks: A survey." Physics Reports, 533(4), 95-142.18

[18] Z. Bahrami Bidoni, R.George, "Discovering Community Structure in Dynamic Social Networks using the Correlation Density Rank," in SocialCom - Stanford, CA, USA. The Sixth ASE International Conference on Social Computing, 2014 19

[19] G. Palla, I. Derényi, I. Farkas, T. Vicsek, "Uncovering the overlapping community structure of complex networks in nature and society," Nature 435 (2005) 814–818.20

[20] S. Kelley, M.K. Goldberg, K. Mertsalov, M. Magdon-Ismail, W. Wallace, "Overlapping communities in social networks," Int. J. Social Comput. Cyber. Phys. Syst. 1 (2) (2011) 135–159.21

[21] S. Zhang, R.S. Wang, X.S. Zhang, "Identification of overlapping community structure in complex networks using fuzzy c-means clustering," Physica A 374 (2007) 483–490.22

[22] I. Psorakis, S. Roberts, M. Ebden, B. Sheldon, "Overlapping community detection using Bayesian non-negative matrix factorization," Phys. Rev. E 83 (2011) 066114.23

[23] A. Lancichinetti, S. Fortunato, J. Kertész, "Detecting the overlapping and hierarchical community structure in complex networks," New J. Phys. 11 (2009) 033015.24

[24] D. Jin, B. Yang, C. Baquero, D. Liu, D. He, J. Liu, "A markov random walk under constraint for discovering overlapping communities in complex networks," J. Stat. Mech: Theory. E 2011.05 (2011) P05031.25

[25] J.B. Huang, H.L. Sun, J.W. Han, B.Q. Feng, "Density-based shrinkage for revealing hierarchical and overlapping community structure in networks," Physica A 390 (2011) 2160–2171.26

 ISBN: 978-1-61208-504-3

[26] J. Xie, S. Kelley, B.K. Szymanski, “Overlapping community detection in networks: the state of the art and comparative study,” ACM. Comput. Surv. (2013) Article No. 43.27

 ISBN: 978-1-61208-504-3

Understanding User-Based Modifications to Information Quality in Response to Privacy and Trust Related Concerns in Online Social Networks

Brian P. Blake and Dr. Nitin Agarwal
University of Arkansas at Little Rock
Little Rock, Arkansas, USA
e-mail: bpblake@ualr.edu nxagarwal@ualr.edu

***Abstract*—As online social networks have surged in popularity, a new wave of privacy discussions are taking place as evolving technology influences perceptions and demands in regard to privacy. From a practitioner's perspective, there is a need to model, measure, and understand information quality in social networks and its relationship to data privacy and trust. From a user's perspective, there is a need to more fully understand both the trust aspects and the visibility and other privacy aspects of information shared online as well as implications from future use of that data. The goal of this research therefore is to model user based modifications to information quality due to data privacy and trust related concerns within online social networks in order to more fully explore the interrelationships and trade-offs between data privacy, trust, and information quality. This research focuses on: 1) development and validation of relationship matrices for data privacy, online social networks, information quality, and trust as a research framework, 2) development of syntax for a conceptual model of data privacy, trust, and information quality in online social networks, and 3) development of a structural equation model for understanding the trade-offs and influences between data privacy, trust, and information quality in online social networks. The greatest implications of this research come through development of integrated matrix frameworks, a privacy/trust/information quality modeling syntax, and structural equation scoring measures that will be applicable to future research efforts. The research will enhance methods of modeling and measuring data privacy, trust, and information quality within online social networks. In application to online social networks, it lends itself to a better understanding of the quality of shared information in given data privacy and trust scenarios. It provides future researchers with a formal framework for relating privacy, trust, and information quality as well as a formal way to understand information quality modification.**

Keywords-Information quality; privacy; trust; online social networks.

I. INTRODUCTION

Social media as communication media have surged in popularity over the past decade. Social networking websites such Facebook, MySpace, and Twitter have been the champions of this social phenomenon [1]. As the use of social media networks increases there are growing concerns about data privacy. A recent paper [2] noted that as information technology evolves it greatly influences perceptions and demands in regard to privacy. Because of this, developments in social computing are driving a new wave of privacy discussions. Government and corporate database privacy issues are often discussed and remain highly important, but according to Zittrain [3] these are "dwarfed by threats to privacy that do not fit the standard analytical template for addressing privacy issues". He used the term Privacy 2.0 to refer to this non-standard view. Zittrain argued that governments or corporations are not always the ones managing surveillance and that control of the transfer of personal information can be eliminated by peer-to-peer technologies.

Frederick Lane, when discussing privacy in a webbed world as part of American Privacy, declared that "information wants to be free" [4]. He continued that social network sites succeed because individuals crave community and will share personal information in order to build it. "Online social networks," he stated, "thrive because they enable us to share personal information more quickly and easily than ever before, creating the impression that we are all newsworthy now". Lane further noted that individuals make seemingly rational decisions to post information online in order to receive perceived benefits, but fully rational decisions require complete information and most individuals don't understand what little control they hold over information posted on social networking sites or personal websites. In a similar vein, Zittrain stated that "people might make rational decisions about sharing their personal information in the short term, but underestimate what might happen to information as it is indexed, reused, and repurposed by strangers" [3].

A. Research Focus

In research related to the general concepts of privacy, trust, and information quality (IQ) each is often addressed in a multi-faceted manner focusing on dimensions, aspects, and properties. To further this, trust, privacy, and information quality as areas of study are interrelated and overlapping in relation to online information disclosure, but how they interact with each other is not fully defined. This is especially true in relation to online social networks (OSNs). Previous research, such as Bertini [5], has noted that there is a direct relationship between privacy, trust, and an individual's willingness to share information of increasing quantity and quality. This creates an opportunity for research. From a practitioners' perspective, there is a need to model, measure, and understand social network information exchanges in regard to privacy, trust, and information quality

 ISBN: 978-1-61208-504-3

trade-offs and modifications. From a users' perspective, there is a need to more fully understand both the trust aspects and the visibility of information shared online as well as implications from future use of that data. The goal of this research therefore is to apply an information quality perspective to the modeling of data privacy within social media networks in order to enable the exploration of the interrelationships and tradeoffs between data privacy, trust, and information quality.

This research will address two problem areas. First, a standard way to frame, model, and measure the relationship of the sub-aspects of data privacy, trust, and information quality to facilitate understanding does not exist. This limits research in relation to a comprehensive understanding and restricts cross-discipline communication. Second, a specific understanding of how information quality modification is used by members of online social networks as a reaction to privacy and trust related concerns has not been fully addressed by the information quality research field. This limits the understanding of outcomes based on existing research models in regard to both antecedent influence and behavioral intentions vs. actual behavior within online social networks from an information quality perspective. A greater understanding of these factors can facilitate online social network organization changes to encourage greater sharing while simultaneously giving a deeper insight into how information is shared from an information quality point of view.

B. Research Implications

The greatest implications of this research will come through development of integrated matrix frameworks, a privacy/trust/information quality modeling syntax, and structural equation scoring measures that will be applicable to future research efforts. The research can enhance methods of modeling and measuring data privacy at both the data element and entity levels. In application to online social networks, it may lend itself to raised awareness of data visibility in social media as well as a better understanding of the quality of shared information in given data privacy and trust scenarios.

C. Structure

The remainder of this paper is organized as follows. Section II describes background issues and related literature. Section III presents research methodologies. Section IV discusses initial results of the research. Section V considers challenges, limitations, and future research opportunities.

II. Background and Related Literature

A. Privacy

According to Daniel Solove in Understanding Privacy [6], nearly 120 years after "The Right to Privacy" by Warren and Brandeis was first published in the Harvard Law Review, current views in the field of privacy form a "sweeping concept" that includes "freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations". He highlighted others who describe privacy as "exasperatingly vague", "infected with pernicious ambiguities", and "entangled in competing and contradictory dimensions". Helen Nissenbaum [7] noted that privacy is commonly characterized in literature as either a constraint on access or a form of control. As theorists conceptualize privacy, they are typically searching for a core common denominator that forms the essence of privacy, but Solove argued that privacy is not easily conceptualized in this manner. He stated that a common denominator approach broad enough to include the varied aspects of privacy is likely to be vague and overly inclusive, while narrower approaches risk being too exclusive and restrictive. Privacy conceptualizations in existing literature can therefore be grouped into targeted common core definitions and broader privacy frameworks.

Major privacy frameworks have been offered by Solove [6], Nissenbaum [7][8], Holtzman [9], and Rössler [10]. From a research perspective, these broader privacy frameworks have a strong structural relationship to the predominant multi-dimensional framework of information quality. Commonalities can be found across most of these privacy frameworks. The sub-components of the Solove and Rössler frameworks have a strong relationship to each other. Generally, sub-components of these frameworks, as Nissenbaum contended, focus around the twin concepts of access and control. In addition, varied determinations and combinations of these framework sub-components will form key aspects of the contextual norms on which Nissenbaum's contextual integrity framework is based.

Solove presented privacy as "a cluster of many distinct yet related things". His privacy framework conceptualization presented in Understanding Privacy organizes privacy into four areas containing related sub-aspects in which privacy concerns have been be historically raised (see Table I). His framework has a strong focus on the collection, processing, and dissemination of information. This aligns well with online social networks and standard information product flows. Solove's framework also aligns well with common multi-dimensional information quality concepts. Because of this, as well as his recognition as a privacy expert, Solove's privacy conceptualization is used as a basis for the privacy aspects of this research.

B. Social Media Networks

Social media is media designed to be disseminated through social interactions created using highly accessible and scalable publishing techniques. It uses internet and web-based technologies to transform broadcast media monologues (one to many) into social media dialogues (many to many). It supports the democratization of knowledge and information, transforming people from content consumers to content producers [11]. Social media networks have been growing in popularity in part due to the increased affordability and proliferation of internet enabled devices that bring social connectivity through personal computers, mobile devices, and internet tablets [12].

 ISBN: 978-1-61208-504-3

Boyd and Ellison [13] describe online social networks as services that enable individuals to "construct a public or semi-public profile within a bounded system", to "articulate a list of other users with whom they share a connection", and to "view and traverse their list of connections and those made by others within the system". Aggarwal [12] states that social networks can be generalized as "information networks, in which the nodes could compromise either actors or entities, and the edges denote the relationship between them". Online social networks are rich in data and provide unprecedented opportunities for knowledge discovery and data mining. From this perspective, there are two primary social network data types. The first type is linkage-based structural data and the second is content-based data. In relation to privacy, Aggarwal highlights three types of disclosure:

> [S]ocial networks contain tremendous information about the individual in terms of their interests, demographic information, friendship link information, and other attributes. This can lead to disclosure of different kinds of information in the social network, such as identity disclosure, attribute disclosure, and linkage information disclosure. [12]

From a more structural perspective, Bruce Schneier [14] proposed that social network data can be divided into six categories (see Table II). Hart and Johnson [15] noted that Schneier's taxonomy highlights three primary sources through which information can be disseminated: through the users themselves, through other individuals, or through inference. In regard to privacy, all three of these sources can lead to privacy compromises. A similar structured view of data is also shared by Facebook [16] in its published data use policy.

TABLE I. A TAXONOMY OF PRIVACY

A Taxonomy of Privacy	
Information Collection	
Surveillance	The watching, listening to, or recording of an individual's activities
Interrogation	Various forms of questioning or probing for information
Information Processing	
Aggregation	The combination of various pieces of data about and individual
Identification	The linking of information to a particular individual
Insecurity	Carelessness in protecting stored information from leaks and improper access
Secondary Use	The use of collected information for a purpose different from the use for which it was collected without the data subject's consent
Exclusion	The failure to allow data subjects to know about the data that others have about them and participate in its handling and use
Information Dissemination	
Breach of confidentiality	Breaking a promise to keep a person's information confidential
Disclosure	The revelation of truthful information about a person that affects the way others judge his or her reputation
Exposure	Revealing another's nudity, grief, or bodily functions
Increased accessibility	Amplifying the accessibility of information
Blackmail	The threat to disclose personal information
Appropriation	The use of the data subject's identity to serve another's aims and interests
Distortion	Disseminating false or misleading information about individuals
Invasions	
Intrusion	Invasive acts that disturb one's tranquility or solitude
Decisional interference	Incursions into the data subject's decisions regarding her private affairs

TABLE II. TYPES OF SOCIAL NETWORK DATA

Types of Social Network Data	
Service Data	Data users give to a social networking site in order to use it
Disclosed Data	What users post on their own pages
Entrusted Data	What users post on other people's pages
Incidental Data	What other people post about a user
Behavioral Data	Data the site collects about user habits by recording what users do and who users do it with
Derived Data	Information about users that is derived from all the other data

C. Information Quality

Information quality (also known as data quality) is a multidisciplinary field with research spanning a wide range of topics, but existing researchers are primarily operating in the disciplines of Management Information Systems and Computers Science [17]. Within quality literature, the concept of "fitness for use" has been widely adopted as a definition for data quality [5][17]-[20]. But in order to be applicable, this definition of fitness for use needs to be contextualized [5]. In this regard, previous writings and research have presented data quality as a multi-dimensional concept [17]-[21].

In 1996, Wang and Strong published a hierarchical framework to capture the multi-dimensional aspects of information quality that are most important to data consumers [19]. This research was presented in application by Strong, Lee and Wang in "Data Quality in Context" the following year [20]. Since that time, their framework has been widely cited in information quality literature. The Wang Strong Quality Framework [19] contains four categories of data quality: Intrinsic DQ, Contextual DQ,

 ISBN: 978-1-61208-504-3

Representational DQ, and Accessibility DQ. These four categories contain fifteen data quality dimensions (see Table III).

TABLE III. WANG STRONG QUALITY FRAMEWORK

DQ Category	DQ Dimensions
Intrinsic DQ	Accuracy, Objectivity, Believability, Reputation
Accessibility DQ	Accessibility, Access Security
Contextual DQ	Relevancy, Value-Added, Timeliness, Completeness, Amount of Data
Representational DQ	Interpretability, Ease of Understanding, Concise Representation, Consistent Representation

D. Trust

Trust, like privacy and quality, is a widely studied concept across multiple disciplines. This has led to the development of a broad array of definitions and understandings of trust over time [22]-[26]. Marsh [22] highlighted that trust values have no units, but can still be measured by such notions as 'worthwhileness' and 'intrinsic value'. At the same time, trust is an absolute medium in which one either trusts or does not trust. This implies that trust in application is based on threshold values above which or below which an entity is either trusted or not trusted as seen in Fig. 1. These thresholds will also vary with different entities and in different circumstances. In a similar manner, Kosa [27] noted that "[t]rust can be examined as a continuous measure, as in evaluation or reliability assessments, or a binary decision point when referring to a decision".

Mayer, Davis, and Schoorman [28] strove to differentiate trust from other related constructs. They presented an integrative model of organizational trust. Within this research, they expanded upon the characteristics of a trustee and presented a concept of perceived trustworthiness. The identified characteristics, or primary factors, of perceived trustworthiness they presented are Ability, Benevolence, and Integrity. In this, Ability relates to the skills, characteristics, and competencies that enable someone to have influence with a specific domain. Benevolence is related to the level of goodwill a trustee is believed to have toward a trustor. Integrity relates to how a trustee is perceived to adhere to an acceptable set of principles. The authors proposed that "trust for a trustee will be a function of the trustee's perceived ability, benevolence, and integrity and of the trustor's propensity to trust". They further noted that, while related, these three attributes are separable and may vary independently of one another.

Gefen [26] drew on concept of trustworthiness presented by Mayer, Davis, and Schoorman to develop a validated scale specifically related to online consumer trust. The results of his research showed that each of the aspects of trustworthiness as tested against online behavioral intentions is different. This may suggest that each of the three aspects of trustworthiness "affect different behavioral intentions because different beliefs affect different types of vulnerability". Gefen's research also illustrated the measurability of aspects such as trust in regard to interactions in an online domain. This is important to the research at hand.

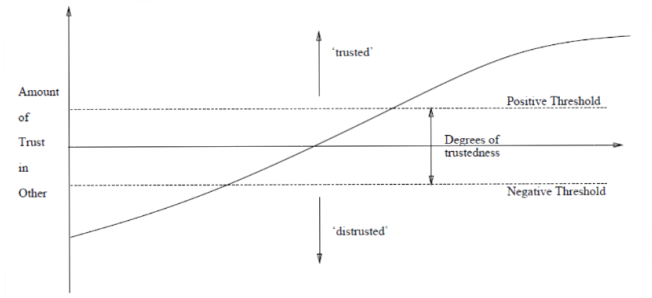

Figure 1 - Positive and Negative Thresholds for Trust [22]

In specific regard to social networks, Adali et al. [29] highlighted that trust also has a major role in the formation of social network communities, in assessing information quality and credibility, and in following how information moves within a network. They further noted the social mechanisms of trust formation in online communities are a new research area and there are many unknowns.

E. Interdependencies

Prior research presented by Bertini [5] begins to highlight the interdependencies between data privacy, trust, and information quality. If quality is defined as fitness for use and accuracy, reliability, and trustworthiness are key aspects of high quality data, then "high quality data require data subjects to disclose personal information raising some threat to their own privacy". Bertini, citing Rose (2001), Hoffman et al. (1999), Neus (2000), and Hui et al. (2006), noted that "studies reveal that data subjects often provide incorrect information or withdraw from interaction when they consider the risks of disclosing personal data higher than the reward they can get from it". As stated previously, control is a key aspect in several conceptualizations and definitions of privacy. Bertini emphasized that lack of control leads to increased concern over "unauthorized secondary use, excessive collection of data, improper access and processing or storing errors". Citing research by Gefen (2002), Paine et al. (2006), and Hoffman et al. (1999), Bertini built on the concept that "[d]ata subjects' level of trust determine both the quantity and the quality of information they disclose" by presenting the relationship between privacy and data quality as a trust mediated process. Bertini noted that the concept of benevolence as presented by Mayer, Davis, and Schoorman is a central trust factor in that both trustee and trustors need to believe that the other is sincere, otherwise data sharing processes breakdown or become cumbersome. He believed that giving users control and allowing them to interact with their data, especially dynamic data, will both increase trust and spontaneously improve data quality. Conversely, when privacy or control is threatened, it causes a loss of trust,

 ISBN: 978-1-61208-504-3

which leads to an immediate decrease in the quality of data being disclosed.

Kosa [27] stated that "research on privacy and trust as linked phenomena remains scarce". She noted that the formalization of trust is much more mature than the formalization of privacy and proposed that because of their conceptual similarities formalization concepts developed in relation to trust could be utilized in the formalization of privacy. Kosa highlights that both trust and privacy are highly information type and sensitivity specific, relationship dependent, purpose driven, and measured on a continuous scale. In example of the application of trust formalizations to privacy, she diagramed, as seen in Fig. 2, proposed thresholds for privacy based on the trust threshold detailed by Marsh [22].

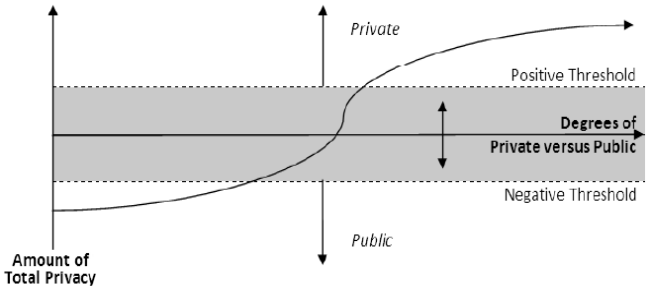

Figure 2 - Proposed Thresholds for Privacy [27]

Further, Kosa presented trust as positively correlated to privacy, but privacy as negatively related to trust. She stated that "Perceptions of trustworthiness may increase the tendency of people to share information willingly, thus giving up their privacy" but the "exercise of privacy may impede trust; if [one chooses] to withhold information, about for example, [his] identity the second party is less likely to trust [him] in the given exchange". This seems counter to the privacy/trust view presented by Bertini [5] above, but it is really a reflection on the relationship of different dimensions between trust and privacy.

For this research, the interdependency between trust, privacy, and information quality as well as the multi-dimensional nature of these concepts highlighted in this section are key foundations. These concepts will be extended in specific relation to online social network sites with a focus on modeling data privacy and measuring the corresponding trade-offs in information quality and/or trust.

III. METHODOLOGY

The research will contain three components that build upon each other. The first will be the development and validation of select relationship matrices for data privacy, online social network data, trust, and information quality as a research framework. The second will be the development of a syntax and conceptual model as a standard way to document the trust, privacy, and information quality aspects within online social networks. Finally, a structural equation model will be developed to measure and validate expected information quality modifications as a reaction to calculated privacy risks based on data elements of different data types, content sensitivity, and data visibility. While these components can be generalized across multiple online social networks, for this research, when analyzing online social networks, Facebook will be used as a primary reference because of the size and activity levels of its user base.

A. Framework Matrix

This research will focus on the general overlap of the multi-faceted dimensions, aspects, and properties of trust, privacy, information quality, and online social networks. It seeks to identify where these areas overlap both in regard to online social networks and to each other. This phase of the research hypothesizes that:

1) The multi-faceted dimensions, aspects, and properties of trust, privacy, and information quality can be effectively overlaid within a series of related matrices.

2) An understanding of intersections of these sub-aspects lends itself to a broader understanding of the relationship of these concepts.

3) An understanding of intersections of these sub-aspects lends itself to specific target areas for future research.

As a starting point for this research, a framework matrix has been developed to map the points of intersection between Solove's [6] taxonomy of privacy, Schneier's [14] divisions of social network data, Wang and Strong's [19] multiple dimensions of information quality, and the trustworthiness characteristics of Ability, Benevolence, and Integrity as presented by Mayer et al. [28] and Gefen [26]. As noted above, the development and validation of select relationship matrices for data privacy, online social networks, information quality, and trust as a research framework will be the first deliverable from this research. This will be accomplished in part through a validation in current literature. Hogben [31], for example, highlighted specific online social network privacy threats that include digital dossier aggregation, secondary data collection, recognition and identification, data permanence, infiltration of networks, profile squatting and ID theft related reputation slander, and cyberstalking/cyberbullying. These can be shown to align neatly with the proposed privacy components within the framework matrix. In addition, a select survey of information quality, online social network, and privacy related professionals and experts whose opinions will be gathered and reconciled.

B. Syntax and Conceptual Modeling

In regard to modeling privacy in social networks, one general approach is the mapping of entity level social graph connections of the network. This high level node and edge view is the most common social graph view. This approach visualizes the issue, but focuses on privacy at the level of overall connections. A second approach presented by Lui and Terzi [32] and others is the calculation of mathematical data element level and entity level privacy scores. This is a

 ISBN: 978-1-61208-504-3

more detailed approach focused on the numeric scoring of data privacy. The concepts of Lui and Terzi were an early influence on the development of this syntax. This research gives the opportunity to blend previous research into an expanded approach. This is done by developing a method to model the data privacy of specific data elements that can then be incorporated in the future into trade-off scoring research. This method may also lend itself in future research to the creation of elemental data privacy social graphs which will allow for the visualization of actual data sharing, not just entity level connections.

The second key aspect of this research is to develop a syntax and conceptual model as a standard way to document the trust, privacy, and information quality aspects within online social networks. This phase of the research hypothesizes that:

1) Instances of trust, privacy, and information quality interactions can be expressed at the data element level in notation sets expressing element, users, privacy, trust, and quality components.

2) Instances of trust, privacy, and information quality interactions can be expressed at the data element level as a conceptual model.

A further research question, if these hypotheses hold true, is whether this be implemented in a way that can aggregate to an overall user level notation and conceptualization. This research will seek to validate these hypotheses through illustration of the conceptual model using synthetic and real world examples as well as validation by extension through structural equation modeling. To control for scope, this research will focus on the user controlled social sharing aspects of online social network information such as Disclosed, Entrusted, and Incidental data rather than organizational (system and third party) aspects such as Behavioral, Derived, and Service data. In this regard, the following syntax structures are being proposed as a concept to be further developed in this research.

For disclosed data elements that users post on their own pages, the most apparent privacy aspect is the visibility level of the data element set by the users' privacy settings. Visibility levels are typically set by users' overall privacy settings or by specific selection when posting a data element. One research question related to this is how trust and information quality are related to a users' determination of visibility related privacy settings. This syntax follows the form of Disclosed Data as D1(J1, PJ1) where D1 = Disclosed Data Element with a descriptive set of J1 = Posting Entity and PJ1 = User Privacy Factors.

For entrusted data elements that users post on other people's pages, there are two main privacy considerations related to the visibility level of the data element. The first is the posting entity's own privacy settings. The second is the receiving entity's privacy settings. Generally, the posting entity's privacy settings are the controlling factor in regard to data visibility. This syntax follows the form of Entrusted Data as E1(J1, J2, PJ1, PJ2) where E1 = Entrusted Data Element with a descriptive set of J1 = Posting Entity, J2 = Receiving Entity, PJ1 = Privacy Factors of the Posting Entity, and PJ2 = Privacy Factors of the Receiving Entity.

For incidental data elements that users post about others, there are also two main privacy considerations. As with entrusted data, the first consideration is the Posting Entity's own privacy settings. This most typically relates to the visibility of the data element. The second consideration is the exclusion factor of the Topic Entity. A Topic Entity is the person, group, or thing which is the subject of a posted data element. Exclusion relates to the level of control and involvement a user has in regard to information that is shared about or actions taken that affect him or her. Within online social networks, this relates to whether or not the incidental data element is directly linked, often through tagging, to the Topic Entity. Topic Entities can often reduce visibility of shared data by preventing tagging or removing tags on incidental data elements, but preventing tagging will increase a user's exclusion factor because the user will be less likely to be directly linked and therefore will not be notified when incidental data is posted. In addition, while a user can reduce visibility by blocking or removing user tags, he or she usually cannot prevent the comments or references themselves from being made by other users. Because of this lack of control, the trustworthiness characteristic of benevolence plays an important role in incidental data. This syntax follows the form of Incidental Data as I1(J1, J3, PJ1, EJ3) where I1 = Incidental Data Element with a descriptive set of J1 = Posting Entity, J3 = Topic Entity, PJ1 = Privacy Factors for the Posting Entity, and EJ3 = Exclusion factor of Topic Entity.

In expansion of this syntax, an important question to be addressed in this research is whether and how quality and trust components such as Q1 as Data Element Quality, TJ1J2/TJ1Jx as Relational Trust between Entities, and TS as System Trust can be incorporated directly into this model syntax. This will need to be developed to facilitate comparative measurement of trade-offs between data privacy, information quality, and trust. This syntax could follow the form of Entrusted Data with Trust and Quality as E1(J1, J2, PJ1, PJ2, TS, TJ1J2, TJ1Jx, QE1) where E1 = Entrusted Data Element with a descriptive set of J1 = Posting Entity, J2 = Receiving Entity, PJ1 = Privacy Factors for the Posting Entity, PJ2 = Privacy Factors for the Receiving Entity, TS = System Trust, TJ1J2 = Relational Trust between Posting and Receiving Entities (subset of TJ1Jx), TJ1Jx = Relational Trust between Connected Entities, and QE1 = Set of Data Element Information Quality Factors (see Fig. 3).

C. Structural Equation Modeling

The goal of the comparative scoring component of this research is to tie the conceptual modeling syntax back to information quality, trust, and data privacy relationships identified in the framework matrices in the first research

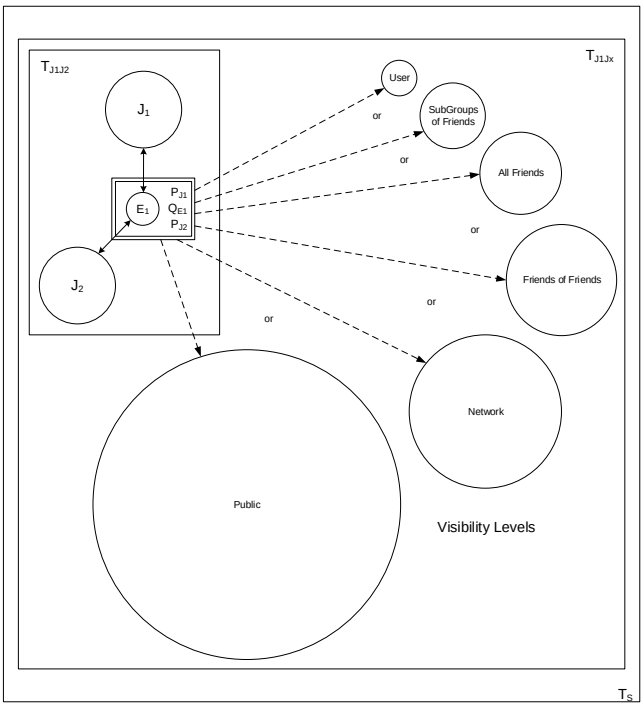

Figure 3 - Data Privacy Modeling of Entrusted Data with Trust and Quality

component. This will have a strong research impact through the creation of a comparative mathematical model of data privacy attributes, information quality dimensions, and trust characteristics. This research phase will develop a structural equation model to measure and validate expected information quality modifications as a reaction to calculated risks based on data elements of different data types, content sensitivity, and data visibility. Previous research showed the benefit of structural equation models in the development and validation of the Internet Users' Information Privacy Concerns [33] and User Privacy Concerns and Identity in OSNs [34] constructs. This research will also use structural equation modeling to extend and build upon those concepts.

Malhotra, Kim, and Agarwal [33] developed the Internet Users' Information Privacy Concerns (IUIPC) construct based on the extension of personal dispositions to data collection, privacy control, and privacy awareness to beliefs regarding trust and risk and how those beliefs affected behavioral intention in regard to Internet usage. This proposed research will extend the IUIPC casual model to online social network specific contextual variables of varied data element type and data sensitivity. It will also incorporate aspects of information quality modification rather than utilize the direct share/not share behavioral intention utilized by Malhotra, Kim, and Agarwal.

Krasnova, Günther, Spiekermann, and Koroleva [34] developed a model for Privacy Concerns and Identity in Online Social Networks (PCIOSN). This cross-discipline research comes more from the social sciences and is developed through a social identity disclosure perspective. They argue that while IUIPC has been widely utilized these applications are lacking because "OSN members are subject to the specific privacy-related risks rooted in the public and social nature of OSNs". They further noted that in terms of primary privacy concerns individuals differentiate between online social network users and provider or third-party organizations. Their research model has a degree of overlap with the proposed framework matrix found in this research. It is based on specific privacy concerns affecting the amount, accuracy, and control aspects of shared information. This research will extend their model to directly map specific privacy and trust aspects from the framework matrix into the threat components of the PCIOSN model. The proposed research will also specifically map dimensions of individual self-disclosure [34] to specific IQ dimensions, as well as incorporate other relevant IQ dimensions, from the proposed framework matrix. Of additional research interest is whether or not the IUIPC and PCIOSN models can be incorporated into a single view through the modeling aspects of this research. This research hypothesizes that:

1) Behavioral intent to share information is not a simple binary response. Instead it is a degree based response that uses information quality modification to mitigate privacy and trust concerns between the thresholds of open disclosure and full non-disclosure (see Fig. 4).

2) Data element types (wall posts, photos, comments, shares, likes, check-ins, etc.) have measurably different thresholds for content sensitivity.

3) Completeness, Accuracy, Accessibility, Amount, Understandability, and similar quality dimensions of shared information are negatively related to calculated privacy and trust concerns as a modification control.

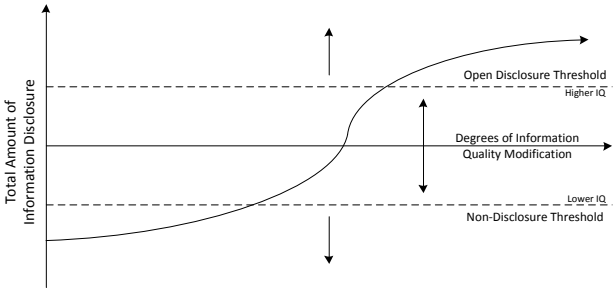

Figure 4 - Initial Information Quality Modification Concept

Hypothesis 1 is an extension of Marsh's Positive and Negative Thresholds for Trust [22] and Kosa's Proposed Thresholds for Privacy [27] as applied to information quality. It should also be noted that any modification of Accessibility IQ dimension mitigates privacy and trust concerns by changing the visibility of a given piece of information rather than changing the shared information itself. As with the second research component, this research will be confined to specific data elements within selected social network data types to control for scope. It will focus first on the user controlled social sharing aspect of Disclosed data, but may easily extend to Incidental and Entrusted data in future research. Specific trust characteristics, information quality dimensions and data privacy aspects will be selected.

 ISBN: 978-1-61208-504-3

For these selected attributes, measurable indicators within online social networks will be identified and corresponding variables and questions for metrics and measurement will be determined. Structural equation modeling will be utilized as a method for measuring the balance trade-offs present between specific trust characteristics, information quality dimensions and data privacy aspects.

IV. CURRENT RESULTS

This paper presents in process doctoral dissertation research. To this point, the relationship matrices for data privacy, online social networks, information quality, and trust as a research framework have been developed and a corresponding validation survey has been created but not yet implemented. Furthermore, an initial syntax for conceptual modeling has been presented. Currently, elements of the proposed structural equation model and its required survey as a validation instrument are under development.

The developed framework matrices are presented in full in Appendices A-D, but as noted in the Section III, only syntax for conceptual modeling of Disclosed, Entrusted, and Incidental data has been developed. This framework matrix subset is presented in Table IV.

TABLE IV. FRAMEWORK MATRIX SUBSET

	Types of Social Networking Data		
	Disclosed Data	**Entrusted Data**	**Incidental Data**
	What you post on your own pages	What you post on other people's pages	What other people post about you
Data Privacy Issues	Increased Accessibility Insecurity Appropriation Secondary Use	Increased Accessibility Secondary use Identification Exclusion Breach of Confidentiality Disclosure Exposure Distortion Intrusion (onto their pages)	Identification Exclusion Breach of Confidentiality Disclosure Exposure Distortion Intrusion (onto your pages) Increased Accessibility Secondary use
Information Quality Dimensions	Accuracy Appropriate Amount Relevancy Security Believability Reputation Understandability Accessibility Objectivity Ease of Operation	Accuracy Appropriate Amount Relevancy Security Believability Reputation Understandability Accessibility Objectivity Ease of Operation	Accuracy Appropriate Amount Relevancy Security Believability Reputation Understandability Accessibility Objectivity Ease of Operation
Trust	Benevolence Integrity	Benevolence Integrity	Benevolence Integrity

Table IV illustrates several key factors. First, intersection points of the matrix may highlight different or similar aspects of privacy, trust, and information quality. Differentiations are shown for only data privacy issues in this subset, but they can be seen more readily in the full framework matrix presented in Appendix A. Second, related social sharing aspects of online social network information such as the user controlled areas of Disclosed, Entrusted, and Incidental data will be more similar to each other than to organizational (system and third party) aspects such as Behavioral, Derived, and Service data. It should also be noted that aspects as currently presented in the matrix intersection points are not in any specific rank order. Even when similar aspects are presented, those aspects may have different levels of importance based on the social networking data type being researched. Finally, the dotted lines found in the data privacy grids for Entrusted and Incidental data are there to indicate distinctions between data privacy violations that may happen to a user and data privacy violations that a user may cause to happen to others.

V. CHALLENGES, LIMITATIONS, AND LOOKING AHEAD

This research faces several challenges and limitations. First, while a broad framework matrix can be presented, the scope for validation and deeper research will be limited to social network data types that relate to user specific aspects of the framework matrix. The role of provider and third-party related online social network data types are highly noteworthy, but they will be addressed in only a limited manner, if at all, in this research. Second, to limit scope during the development of a syntax and conceptual model, not all variations of data element types and entity interactions will be addressed. Once again, in order to control research scope, the focus will be on select user specific aspects of the framework matrix as well as a targeted set of matrix overlays. This series of scope limitations is detailed more specifically within the Methodology section of this paper.

Challenges for this research may include determining and attracting a diverse set of respondents to create a representative population in phase three of this study. For measurements within structural equation modeling to be considered valid certain minimum respondent thresholds need to be met based on the number of components within the model. In addition, structural equation modeling analysis requires the identification of alternate models. Because of the dynamics of social networks, identifying all alternative models may be difficult. Further, finding field experts willing to participate in the framework matrix validation survey may also be difficult, but since only a small number are required it may be a challenge that is more easily overcome.

REFERENCES

[1] B. Blake, N. Agarwal, R. Wigand, and J. Wood, "Twitter Quo Vadis: Is Twitter Bitter or are Tweets Sweet?" The Seventh International Conference on Information Technology: New Generations (ITNG), 2010, pp. 1257-1260.

[2] K. Borcea-Pfitzmann, A. Pfitzmann, and M. Berg, "Privacy 3.0 := Data Minimization + User Control + Contextual Integrity," it - Information Technology, vol. 53, no. 1, pp. 34-40, 2011. [Online]. Available from: https://tu-dresden.de/Members/katrin.borcea-pfitzmann/ 2016.07.16

 ISBN: 978-1-61208-504-3

[3] J. Zittrain, The Future of the Internet - And How to Stop it, New Haven, CT: Yale University Press, 2008.

[4] F. S. Lane, American Privacy: The 400-Year History of our Most Contested Right, Boston, MA: Beacon Press, 2009.

[5] P. Bertini, "Trust Me! Explaining the Relationship Between Privacy and Data Quality," Information Technology and Innovation Trend in Organization, 2010. [Online]. Available from http://www.cersi.it/itais2010/ 2016.07.16

[6] D. J. Solove, Understanding Privacy. Cambridge, MA: Harvard University Press, 2008.

[7] H. F. Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford, CA: Stanford University Press, 2010.

[8] H. Nissenbaum, Privacy as contextual integrity. *Washington Law Review*, vol. *79*, no. 1, pp. 101-139, 2004. Available from http://www.nyu.edu/projects/nissenbaum/main_cv.html#pub 2016.07.16

[9] D. H. Holtzman, Privacy Lost: How Technology is Endangering Your Privacy, San Francisco: Jossey-Bass, 2006.

[10] B. Rössler (Ed.), Privacies: Philosophical Evaluations, Stanford, Calif: Stanford University Press, 2004.

[11] N. Agarwal, Types of Social Media, lecture presented for Social Media Mining and Analytics course at the University of Arkansas at Little Rock, Feb. 2011.

[12] C. C. Aggarwal, Social Network Data Analytics, New York: Springer, 2011.

[13] D. M. boyd and N. B. Ellison, "Social Network Sites: Definition, History, and Scholarship," Journal of Computer-Mediated Communication, vol. 13, no. 1, pp. 210-230, 2008.

[14] B. Schneier, "A Taxonomy of Social Networking Data," IEEE Security & Privacy Magazine, vol. 8, no. 4, p. 88, 2010, doi: 10.1109/MSP.2010.118

[15] M. Hart and R. Johnson, "Prevention and Reaction: Defending Privacy in the Web 2.0," 2010. [Online]. Available from: http://www.w3.org/2010/policy-ws/papers/04-Hart-stonybrook.pdf 2016.07.16

[16] Facebook, Data Policy, [Online]. Available from: https://www.facebook.com/about/privacy/your-info 2016.07.16

[17] S. E. Madnick, R. Y. Wang, Y. W. Lee, and H. Zhu, "Overview and Framework for Data and Information Quality Research," Journal of Data and Information Quality, vol. 1, pp. 2:1-2:22, 2009.

[18] C. Fisher, E. Lauria, S. Chengalur-Smith, R. Wang, Introduction to Information Quality, M.I.T. Information Quality Program, 2006

[19] R. Y. Wang and D. M. Strong, "Beyond Accuracy: What Data Quality Means to Data Consumers," Journal of Management Information Systems, vol. 12, no. 4, pp. 5-33, 1996.

[20] D. M. Strong, Y. W. Lee, and R. Y. Wang, "Data Quality in Context," Commun. ACM, vol. 40, pp. 103-110, May 1997.

[21] L. L. Pipino, Y. W. Lee, and R. Y. Wang, "Data Quality Assessment," Commun. ACM, vol. 45, pp. 211-218, Apr. 2002.

[22] S. P. Marsh, Formalising Trust as a Computational Concept, unpublished doctoral dissertation, University of Stirling, 1994. [Online]. Available from: https://dspace.stir.ac.uk/ 2016.07.16

[23] C. D. Schultz, "A Trust Framework Model for Situational Contexts," Proceedings of the 2006 International Conference on Privacy, Security and Trust: Bridge the Gap between PST Technologies and Business Services (PST '06), New York, NY, USA: ACM, 2006, pp. 50:1-50:7.

[24] D. McKnight and N. Chervany, "Conceptualizing Trust: A Typology and E-commerce Customer Relationships Model," Proceedings of the 34th Annual Hawaii International Conference on System Sciences, 2001, p. 10.

[25] A. Gutowska, Research in Online Trust: Trust Taxonomy as a Multi-Dimensional Model, Technical Report, School of Computing and Information Technology, University of Wolverhampton, 2007.

[26] D. Gefen, "Reflections on the Dimensions of Trust and Trustworthiness Among Online Consumers," SIGMIS Database, vol. 33, pp. 38-53, 2002.

[27] T. Kosa, "Vampire Bats: Trust in Privacy," Eighth Annual International Conference on Privacy Security and Trust (PST), 2010, pp. 96-102, doi: 10.1109/PST.2010.5593227.

[28] R. C. Mayer, J. H. Davis, and F. D. Schoorman, "An Integrative Model of Organizational Trust," The Academy of Management Review, vol. 20, no. 3, pp. 709-734, 1995.

[29] S. Adali, R. Escriva, M. K. Goldberg, M. Hayvanovych, M. Magdon-Ismail, B. K. Szymanski, and G. Williams, "Measuring Behavioral Trust in Social Networks," 2010 IEEE International Conference on Intelligence and Security Informatics (ISI), 2010, pp. 150-152.

[30] D. L. Hoffman, T. P. Novak, and M. Peralta, "Building Consumer Trust Online," Commun. ACM, vol. *42*, pp. 80-85, Apr. 1999.

[31] G. Hogben (Ed.), ENISA Position Paper No. 1: Security Issues and Recommendations for Online Social Networks, European Network and Information Security Agency, Nov. 2007. [Online]. Available from: https://www.enisa.europa.eu/publications/archive/security-issues-and-recommendations-for-online-social-networks 2016.07.16

[32] K. Liu and E. Terzi, "A Framework for Computing the Privacy Scores of Users in Online Social Networks," Ninth IEEE International Conference on Data Mining (ICDM '09), 2009, pp. 288-297, doi: 10.1109/ICDM.2009.21.

[33] N. K. Malhotra, S. S. Kim, and J. Agarwal, "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," Information Systems Research, vol. 15, no. 4, pp. 336-355, 2004. doi: 10.1287/isre.1040.0032.

[34] H. Krasnova, O. Günther, S. Spiekermann, S., and K. Koroleva, "Privacy Concerns and Identity in Online Social Networks," Identity in the Information Society, vol. 2, no. 1, pp. 39-63, 2009, doi: DOI 10.1007/s12394-009.

 ISBN: 978-1-61208-504-3

APPENDIX A - FRAMEWORK MATRIX: INFORMATION QUALITY, DATA PRIVACY, AND TRUST IN SOCIAL MEDIA NETWORKS

	Types of Social Networking Data					
	Service Data	**Disclosed Data**	**Entrusted Data**	**Incidental Data**	**Behavioral Data**	**Derived Data**
	Data you give the social network site in order to use it	What you post on your own pages	What you post on other people's pages	What other people post about you	Data the site collection about your habits by recording what you do and who you do it with	Data about you that is derived from all other data
Data Privacy Issues	Insecurity Secondary use Breach of Confidentiality	Increased Accessibility Insecurity Appropriation Secondary Use	Increased Accessibility Secondary use Identification Exclusion Breach of Confidentiality Disclosure Exposure Distortion Intrusion (onto their pages)	Identification Exclusion Breach of Confidentiality Disclosure Exposure Distortion Intrusion (onto your pages) Increased Accessibility Secondary use	Aggregation Insecurity Secondary Use Breach of Confidentiality Identification Exclusion	Aggregation Insecurity Secondary Use Breach of Confidentiality Identification Exclusion
Information Quality Dimensions	Accuracy Appropriate Amount Relevancy Security Accessibility Concise Representation Consistent Representation	Accuracy Appropriate Amount Relevancy Security Believability Reputation Understandability Accessibility Objectivity Ease of Operation	Accuracy Appropriate Amount Relevancy Security Believability Reputation Understandability Accessibility Objectivity Ease of Operation	Accuracy Appropriate Amount Relevancy Security Believability Reputation Understandability Accessibility Objectivity Ease of Operation	Accuracy Appropriate Amount Relevancy Security Timeliness Concise Representation Completeness Consistent Representation Accessibility Understandability Interpretability	Accuracy Appropriate Amount Relevancy Security Accessibility Understandability Interpretability Consistent Representation Concise Representation
Trust	Ability Benevolence Integrity	Benevolence Integrity	Benevolence Integrity	Benevolence Integrity	Ability Benevolence Integrity	Ability Benevolence Integrity

APPENDIX B - FRAMEWORK MATRIX: DATA PRIVACY AND INFORMATION QUALITY

	Types of Data Privacy Issues					
	Information Processing					
	Aggregation	Identification	Insecurity	Secondary use	Exclusion	
Information Quality Dimensions	Accuracy Appropriate Amount Relevancy Believability Timeliness	Accuracy Believability Reputation	Security Accessibility	Appropriate Amount Accessibility Security Relevancy Accuracy	Security Accessibility Understandability Interpretability Timeliness	
	Information Dissemination					
	Breach of Confideniality	Disclosure	Exposure	Increased Accessibility	Appropriation	Distortion
Information Quality Dimensions	Reputation Accuracy Believability Accessibility	Reputation Believability Accuracy Accessibility Appropriate Amount Relevancy	Reputation Believability Accuracy Accessibility Appropriate Amount	Accessibility Security Appropriate Amount	Security Reputation Believability Accuracy	Reputation Believability Accuracy Accessibility
	Invasions					
	Intrustion	Decisional Interference				
Information Quality Dimensions	Security Accessibility Appropriate Amount	Security Accessibility Appropriate Amount				

APPENDIX C - FRAMEWORK MATRIX: DATA PRIVACY AND TRUST

	Types of Data Privacy Issues					
	Information Processing					
	Aggregation	Identification	Insecurity	Secondary use	Exclusion	
Trust	Ability Benevolence Integrity	Ability Benevolence Integrity	Ability Benevolence Integrity	Benevolence Integrity	Benevolence Integrity	
	Information Dissemination					
	Breach of Confideniality	Disclosure	Exposure	Increased accessibility	Appropriation	Distortion
Trust	Benevolence Integrity	Benevolence Integrity	Benevolence Integrity	Ability Benevolence Integrity	Benevolence Integrity	Benevolence Integrity
	Invasions					
	Intrustion	Decisional Interference				
Trust	Ability Benevolence Integrity	Ability Benevolence Integrity				

APPENDIX D - FRAMEWORK MATRIX: TRUST AND INFORMATION QUALITY

	Characteristics of Trust		
	Ability	Benevolence	Integrity
Information Quality Dimensions	Accessibility Timeliness Ease of Operation	Objectivity Reputation Appropriate Amount Relevancy Accuracy Completeness	Believability Reputation Objectivity

 ISBN: 978-1-61208-504-3

Blockchain:

The Emergence of Distributed Autonomous Institutions

Mariusz Nowostawski

Norwegian University of Science and Technology
Gjøvik, Norway
Email: mariusz.nowostawski@ntnu.no

Christopher K. Frantz

Otago Polytechnic
Dunedin, New Zealand
Email: cf@christopherfrantz.org

***Abstract*—We present a novel institutional perspective on the distributed consensus and ledger technology known as *blockchain*. We discuss the concept of *Distributed Autonomous Institutions* that are able to facilitate global interactions, contracts, and value transfers, all of which are achieved without the need for the human-based third party trust. We argue that due to its properties and design blockchain technology represents a disruptive change in the modelling paradigms of socio-technical systems. Distributed trust and consensus mechanisms offered by blockchain technology represent a novel, qualitatively different, phenomenon. We present the general design principles, stakeholders, the dynamics between those stakeholders, the incentive models, and the consensus protocols currently used in blockchains, before highlighting the potential of blockchain technology to develop distributed autonomous institutions. We conclude with a discussion of challenges associated with the adoption of blockchain technology.**

Keywords–blockchain; governance; autonomy; distributed autonomous institutions; public ledger; mining; consensus; smart contracts; Bitcoin; DashCoin; Ethereum

I. INTRODUCTION

One of the important enablers for modern civilization has been the invention of language. Spoken language has enabled the evolution of complex, yet stable communication patterns [1], whereas written language has provided persistence [2] and added the ability to communicate asynchronously, sometimes across centuries or millennia. Communication and persistence have further played a fundamental role in the development of modern computing paradigms. Since the invention of the von Neumann architecture, human development and institutional automation has accelerated, as evidenced in increasingly complex forms of social and economic organisation and associated regulation. Example phenomena include the increasing numbers of digital nomads and flexible organisational boundaries based on procurement of external services. We claim that the accelerated development and growth in complexity in human institutions ultimately relies on the three fundamental elements: (1) *communication*: the ability to communicate and synchronize; (2) *persistence*: the ability to store communication or data; and (3) the *ability to compute*: ie. automatically execute an algorithm, or in other words, a finite set of computational steps. This parallels the characteristics of what we refer to as institutions [3], or "manifestations of social behaviour" [4], which are characterised by (a) *social interaction*, (b) *stability*, i.e., institutions' ability to survive the constituting behaviour [5], and (c) *procedural prescription* of desirable behaviour (or proscription of undesirable behaviour) that may or may not be explicitly codified [6] (e.g., as laws vs. social norms). While the internet enabled communication across organisational and national boundaries, laying the foundation for modern virtual organisations, its primary focus was the facilitation of general human communication. The actual state was held within the endpoints, not the network itself. Only the introduction of peer-to-peer technology in the early 2000s (e.g., [7]) moved state into the network itself. Thus state did no longer rely on individual endpoints, but was rather distributed across a collection of participating network nodes. Therefore, the state could be managed in the network itself, the modification required explicit intervention by individual nodes based on externally negotiated semantics. In this context 'externally negotiated' implies that the higher-level application-specific semantics (beyond the primitive CRUD operations Create, Read, Update and Delete) are not managed by the system itself. Even though cloud technology reinforced the virtualisation and decentralisation of computation, it did not change the institutional status: the control is retained with a single well-defined entity, generally the owning organisation. The inability to delegate the guaranteed execution of complex instructions, along with assurance of transaction safety to the network itself, limits the adoption for critical services outside the control of organisations such as banks, insurances and governments. We argue that the final missing pillar, the *decentralised execution of procedural prescriptions* makes all the difference in building truly open institutional environments, enabling us to relay critical coordination tasks, such as digital payments, tendering of governmental contracts, or even democratic voting processes to the network itself. Table I summarises the institutional properties of the highlighted technologies.

TABLE I. INSTITUTIONAL CHARACTERISTICS AND ASSOCIATED ENABLING TECHNOLOGY

Technology	Communication	Persistence	Distributed Computation
Internet	•		
P2P Technology	•	•	
Blockchain	•	•	•

We believe that *blockchain technology* reflects the natural evolution towards loosely coupled, user-centric, distributed and autonomous institutions, that will fundamentally change

 ISBN: 978-1-61208-504-3

the nature in which humans engage with computers, and, in extension, with other humans. In this context the autonomous nature of institutions reflects the continuous operation without the need for any human intervention.

In Section II we briefly introduce the principles that underlie blockchain technology and highlight the central characteristics that produce the added value that has the potential to redefine the modern economic landscape. We further introduce Bitcoins and DashCoins as example implementations of blockchain technology, before introducing the more advanced blockchain-enabled decentralised computation in Section III. In Section IV, we introduce the concept of *Distributed Autonomous Institutions*, before discussing their impact on socio-technical systems as well as society in the wider sense in Section V, along with an outlook on future work.

II. BLOCKCHAIN

Blockchain technology facilitates the fundamental shift based on automated, yet flexible mechanisms that deal with trust and liability based on adaptive incentive systems. The underlying cornerstone of public blockchain technology is solving the consistency problem, that is, ensuring a consistent indisputable representation of state and transitions outside of the control of either single stakeholder. The mathematical consistency of events, or transactions, is assured by aligning the incentive model with the goals of the distributed network of peers. In this context 'public' implies that blockchain applications operate in the open public sphere and coordinate interaction between unknown participants in a permissionless fashion, i.e., in principle anyone can participate.

Whereas the distributed nature of state is unproblematic, its synchronised modification is. In an open distributed environment all the nodes need to achieve consensus about whether an individual transaction is accepted or rejected. Accepted transactions must be subsequently integrated into the shared chain of transactions held within the blockchain. Decision-making generally operates based on social choice protocols, such as voting (e.g., majority-based voting). Thus stakeholders cannot modify the distributed shared state or cheat without collaboration by the majority of other stakeholders. The probability of colluding is reduced by network size and anonymity, as well as ensuring that cheating carries a risk of value loss. In this context *value loss* means waste of computational resources or loss of the managed resources, e.g., digital currency. However, any modification puts a computational burden on all members of the network. This aspect could be exploited by injecting large numbers of transactions and reducing the blockchain's ability to process those, while maintaining global consistency. The associated expectation is that fraudulent transactions (e.g., declaring multiple transactions of the same funds at the same time) will be accepted by a critical number of hosts and eventually be accepted into the global blockchain. In the absence of a central sanctioning authority, blockchain modifications (i.e., transactions) need to be cheap enough not to discourage the system's use, yet expensive enough to prevent opportunistic abuse (e.g., by submitting fraudulent transactions). Mechanisms that facilitate this trade-off include the consumption of high amounts of processing power or per-transaction payments. This balance of incentive and deterrence is the *proof of work* [8]. An alternative approach that avoids the inefficiencies associated with the proof of work, such as wasted power and processing time, as well as to limit the computational 'arms race' for computing power, is the *proof of stake*. In the proof of stake [9] the individual participants' influence is constrained by their commitment to the system, such weighing the influence by the amount of resources individual participants hold. Naturally, this introduces hierarchical characteristics into the system, but increases the efficiency of the system without unproductive use of computing resources. Whatever the specific protocol employed by a given blockchain implementation, the proof of work, proof of stake, and the voting model used for validation work in unison; the stable long-term strategy is not to cheat. Decentralised blockchain technology offers third-party trust without any single entity taking the full responsibility or having full authority.

What this means for institutional settings [10] is that trust and liability can now be flexibly shifted on a spectrum ranging between the institution itself and the participating individuals. Let us take an example of a simple asset, e.g., a currency. Let us assume that selfish individuals only trust themselves completely, i.e., one cannot cheat or misuse one's own trust. Being a custodian of one's own assets carries liability, e.g., for safekeeping. To relieve oneself from the liability, one can give custody of the asset to a trusted institution (Institution **A** in Fig. 1), such as a bank. Once an individual deposits an asset, the bank is liable for the safety and security of that deposit. The liability has been transferred from the individual to the institution. However, that transfer also introduces the need for trust. The individual must now put their trust in the bank.

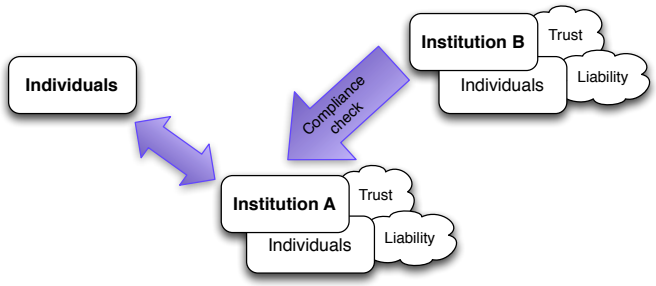

Figure 1. Trust Relationships in the Traditional Institution Concept

To relieve one from liability, and to pass the liability to the bank, one thus has to trust the bank, or, more precisely, institutions that regulate and control the bank's operation (Institution **B** in Fig. 1), since the inner workings are inaccessible to trusting individuals and are thus not openly verifiable. But what if one trusts none but oneself, but still wants to pass the reliability to an institution? The solution is a *Decentralised Autonomous Organisation* (DAO) [11] – an algorithm, that codifies the participants, governed resources as well as protocols. The algorithm that is guaranteed to work according to its specification and, if well constructed, never fails. Once instantiated, it would thus never break the trust one puts into it, since the algorithm exhibits verifiable trust. Therefore, with the blockchain it is possible to achieve the liability transfer from individual to institution, without the putting trust into a traditional institution that operates based on human intervention (e.g., a notary). That said, any DAO can only be as good as its implementation. A DAO is governed by verifiable code and reliable execution, but that does not

 ISBN: 978-1-61208-504-3

protect it against bugs introduced at design time. A good example for the importance of thorough development is the recent exploitation of the most prominent DAO and the theft of around one third of all entrusted funds [12].

As another example for a blockchain-enabled application, consider a simple escrow service. Typically, an escrow service is used to assure atomicity of a transaction between two non-trusted entities, and to have the ability to roll back a partially fulfilled transaction. An escrow service, a trusted third party is used to work as a trusted intermediary to facilitate the transaction. With the blockchain, such transactions are atomic by design, without the need for a trusted third party. What those examples demonstrate is that many centrally-managed services, in particular those provided by insurance companies, banks, or governments, can be made more secure and more transparent with the use of blockchain technology. This means that the human element can be eliminated from selected institutions or contractual agreements, especially in areas in which the ability to maintain accountability is challenging. This has a fundamental impact on how we will perceive and deal with fraud, data leaks or power abuse. This potential and the associated challenges become clearer when exploring examples of blockchain technology with respect to structural and governance characteristics. In the following subsections we thus highlight some examples of blockchain technologies to illustrate the sketched potential.

A. Bitcoin

The first deployment of the blockchain technology and currently the most dominant virtual currency is known as Bitcoin. The creator of the system, known as Satoshi Nakamoto, wrote about the system in a founding white paper [13]. The global network of *miners* and users is one of the largest and most powerful computational resources currently in operation.

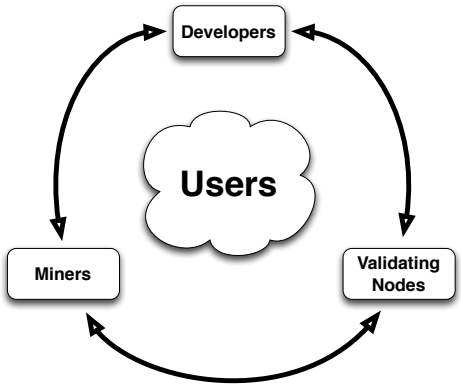

Figure 2. Blockchain Stakeholders

Stakeholders. At its essence the Bitcoin network relies on two operations, a) the *mining* of the currency (i.e., production or minting of the currency tokens), and b) the *validation* of transactions (i.e., facilitating the use of the currency). This is mediated by a set of stakeholders, a schematic overview of which is depicted in Fig. 2. The *developers* provide code for the mining and the consensus library. The *miners* generate new blocks that contain the individual transactions. The *validating nodes* run software to accept or reject transactions. In addition, validating nodes also accept or reject blocks mined by the miners. To regulate individual influence, the acceptance relies on majority-based voting between the validating nodes. The detailed workings of the system are further explained in [13] and in [14].

Instead of exploring the technical complexity here, we only focus on the circular dependencies between all three stakeholders. Validating nodes are not able to influence the process alone, because they lack the computational power necessary to compute the blocks. Miners, who possess the necessary computational resources, are not capable of influencing the voting process directly, as the network of validating nodes is larger than the mining network. This makes it difficult to obtain 51% of voting power. The developers shape the rules and the consensus protocol, but can neither control the mining nor the network. In principle, all parties thus have a strong incentive to maintain the trust and operational integrity of the network, without the risk of any other group exerting full control, thus giving the system characteristics of a *common pool resource* [15] with distributed governance.

Centralisation. In the early days of the deployment the users of Bitcoin used to be the ones running the mining as well as contributing their computing resources as validating nodes. That was the initial assumption of Satoshi, and mining as well as validating was built into the Bitcoin wallet software. The goal was to keep the network as large and as distributed as possible. However, over time an interesting phenomenon occurred, similar to the development of internet services: centralisation. Due to increased popularity of simplified wallets, increased demands on storage and traffic to maintain fully validating nodes, and the escalation of computational resources needed for mining, most contemporary Bitcoin users are neither miners nor validating nodes. This model has severe limitations, and the community has yet to work out how to address the increase in centralisation of the system. A related phenomenon that exemplifies the complexity of influence factors on the structural characteristics of the network is the fact that majority of mining power for Bitcoin now resides in China [16]. A reason for this lies in the exceptionally cheap access to electricity and the direct access to the mining hardware that is produced in China. Thus micro-economical incentives have tangible impact on the network structure itself. The other property of Bitcoin is that it does not control who the miners or who the validating nodes are. The network can be infiltrated by malicious nodes in an attempt to destabilise the network, or simply to monitor the transactions in order to de-anonymise network participants [17], an aspect we will discuss in the following.

Anonymity and Traceability. Anonymity in Bitcoin network takes a weak form of pseudonymity. That implies that users' identities are hidden behind pseudonyms that can be tracked through the blockchain. Bitcoins are not fungible. Fungibility is the property of a good or a commodity such that its units are completely interchangeable, and can be easily substituted. The Bitcoin protocol allows traceability of transactions between the pseudonyms, and as soon as a given pseudonym is attached to a real person, there is a possibility of de-anonymising other transaction participants. In order to maintain anonymity, specially crafted mixing services need to be used to make tracking harder, or statistically impossible. Those services work in such a way that they generate a large

 ISBN: 978-1-61208-504-3

number of bogus transactions that obfuscate the true coin ownership in the transaction graph.

Governance. From a socio-technical perspective, the most interesting element of the Bitcoin blockchain is its governance model, or, to be precise, the lack of it. The network is fully self-organising, and there is no governance model built in. The decision making and protocol refinement happen through iterative decision-making processes and community adoption. In theory, it means progress can be achieved by the community through majority-based voting. In reality, due to lengthy iterations between the discussions, development, and partitioning of the development efforts, the progress and adoption of ideas is slow. With focus on the reliability and long-term viability of the currency, this can be a desirable property, since it is based on the democratic consensus-based decision-making. On the other hand, consensus-building involves an inherent risk of community partitioning, or even a *hard fork*. A hard fork occurs if the community and the network splits into two chains, out of which one is likely not to persist in the long term. This means assets stored in the eventually discontinued fork are ultimately lost. However, hard forks can occur intentionally: Ethereum's (see Section III) recent funds theft led to precisely that decision based on community consensus [18] in an attempt to revert the fraudulent transactions.

B. DashCoin

To address some of the shortcomings of the original Bitcoin structure, alternative currencies have emerged. One example for this development are DashCoin, whose structural characteristics we will compare to Bitcoin, in order to disambiguate blockchain technology from specific applications built on its principles.

Stakeholders. The Dash network is fundamentally similar to the Bitcoin network. However, there are some interesting modifications. The Dash protocol introduces a concept of *second layer* nodes, called *master nodes*. Those are selected nodes that provide a certain proof of stake, or collateral, such that only a limited amount of nodes ever exist in the network. Those nodes are rewarded for participating in the network and they provide certain services, such as governance and voting on new services, allocation of funds, and consensus rules. Those nodes can also provide a distributed oracle service, that is, provide a verifiable ground truth without the need for a trusted third party. Because there is a limited amount of those, and the fact that they can be verifiably trusted (due to the collateral that they deposit), certain operations, such as the confirmation of transactions, can be done much faster than in the Bitcoin model.

Centralisation. The Dash network addresses the issues of centralisation by delegating some of the duties to second-tier nodes (master nodes). The number of those is kept within the range of 3500-4000 nodes, which is sufficient to sustain a robust network. Each of those nodes has deposited 1000 DASH, which means those are core stakeholders in the network, whose incentives are aligned with the group incentives as a whole. Besides the proof of stake, the network also employs a proof of work algorithm that bears no benefits if implemented in hardware – anyone can participate in mining using their graphics processing unit (GPU), and it is not beneficial to implement the algorithm in hardware (e.g., in application-specific integrated circuits (ASICs)).

Anonymity. Coins can be passed in pseudo-anonymous fashion, similar to the Bitcoin. However, there is a built-in transfer mode that mixes the coin in transit, using the master nodes for this purpose. Therefore, the coins can be transferred in statistically anonymous fashion without the need for additional services.

Governance. The most interesting feature is the governance model, consisting of the group of major network stakeholders, i.e., the master nodes. Each master node has the right to vote on resolutions and the majority of voters decide on the structure and future of the network itself. Due to the design, the objectives of the network as a whole, its customers/users, and the master node operators are aligned to promote privacy, consistency, and security. The Dash network does not suffer any of the limitations of the Bitcoin blockchain governance.

C. Example Applications

Fully anonymous, atomic, and reliable peer-to-peer transfer of value is one of the most common examples of the blockchain technology application. It offers the potential to facilitate fully automated micro payments and full remittance automation. Due to built-in mechanisms for delayed payment and multi-party signatures, it is possible to build more complex contractual agreements between parties, and involve multiple participants in the value transfer. Bitcoin and Dash blockchains can be used to issue digital assets, or work as a public registry of ownership (e.g., land title management [19]). Recent developments include prospective adoption of blockchain technology to regulate insurance subsidies based on real-time risk pooling [20]. Alternative use cases involve decentralised identity management [21], or the use of the blockchain to verify and validate the existence of documents based on their hash, without making the actual content public [22]. Despite the novelty of those approaches, all applications share the public ledger concept as the essential operational principle.

III. Decentralised Computation

Existing public ledgers, such as the Bitcoin blockchain, provide a decentralised, verifiable and mathematically consistent transaction tracking. Each newly created transaction is atomic, that is, it is either fully included into the chain, or it is discarded. This is similar to a distributed database system. The difference being that everyone can participate in maintaining that database, and there is no single central authority that dictates the rules.

The computational expressiveness of such a ledger is limited to several cryptographic operations. This has been a carefully chosen design decision to keep the computational complexity of validating and verifying transactions simple, so as to ensure broad participation. However, this effectively limits the computational capabilities of the ledger itself. Any state transitions or computations that do not use crypto-primitives must be executed by a trusted third party.

Ethereum [11] takes the next incremental step towards automating institutions. It has been designed from ground up to enable execution of arbitrary, Turing-complete code *within* the transaction itself, making it a distributed ledger and distributed execution environment at the same time. This means that the blockchain itself can host a transparent and inspectable process: a sequence of steps that express an algorithm, or state machine transitions that are monitored and executed by

 ISBN: 978-1-61208-504-3

the network itself. The user who wishes to invoke the logic must remunerate the network for the execution of all the operations. No single node or potentially inconsistent client implementations can be held responsible for executing that computation. Though the collective of nodes provides the computational capabilities, the computation itself is distributed across those nodes and cannot be unilaterally modified or prevented. To prevent or circumvent the execution, the entire network would have to be taken down, the prospect of which is unrealistic once a critical adoption level is reached. Going beyond the sovereignty-agnostic currency flow enabled by cryptocurrencies like Bitcoin and DashCoin, this means that specific executions do no longer underlie a single determinable jurisdiction, making the execution truly distributed in the sense of transparency and fungibility.

In practice, the system relies on *ether* (and its subdenomination *wei*) as fundamental unit of exchange that is needed to pay for deploying code. Ether is generated by miners but can be procured via exchanges. The users specify contracts, which can be as simple as modifiable objects, or as complex as long-running decision-making processes, like voting or deploying one's own cryptocurrency inside the Ethereum network. The required payment (*gas*) is estimated based on code complexity and charged to the deploying party. Contracts, or *smart contracts*, are created using the companion Javascript-inspired programming language Solidity [23]. Solidity allows the specification of a contract's stakeholders, permissible modifications, execution conditions (e.g., triggers for voting) as well as termination conditions. Deployed contracts are uniquely identified and publicly visible. The required remuneration for contract deployment deters from excessive use and is deposited during deployment. Unused funds are reimbursed if the initial projection was too high.

The new quality of automated enforcement of codified contracts highlights the importance of thorough development and testing, an aspect that has become evident in the recent first massive hack of an Ethereum DAO [12]. But in this young and dynamic field, solutions are already on the horizon. A proposed solution to this problem is the use of child chains to coordinate asset-based transactions as implemented in the new blockchain alternative Ardor/NXT 2.0 [24], which is under development and to be released for production use in 2017. In contrast to Ethereum's support for general-purpose code, Ardor will concentrate on specific asset-based transactions. The concept of child chains permits the delegation of specified operations onto a given sub chain, and thus increasing the security by limiting the visibility to relevant stakeholders. The security model is further strengthened by supporting complex preconditions for the execution of transactions. In addition, the delegation to child chains increases the scalability of the entire network by reducing the necessary decentralised computations. The concept furthermore includes built-in mechanisms to manage governance and decision-making processes in a reliable and anonymous fashion.

However the blockchain landscape will develop in the future, we see specifically the delegation of code execution into the blockchain itself as the game-changing feature, and the foundation of what we refer to as *Distributed Autonomous Institutions*. Table II provides an overview of essential institutional functions as performed in the discussed instances of blockchain technology.

TABLE II. BLOCKCHAIN TECHNOLOGY INSTANCES AND DISCUSSED CHARACTERISTICS

Technology	Validation	Governance	Managed Artefacts/ Capabilities
Bitcoin	majority-based voting	informal community-based	transactions
DashCoin	stake-based representative voting		transactions
Ethereum	majority-based voting	informal community-based[a]	transactions & stateful autonomous code execution

[a] The community-based governance system is currently undergoing revision in the light of the recent DAO theft, with directions pointing towards the explicit appointment of governing entities based on constitutional principles (see e.g., [25]).

IV. Distributed Autonomous Institutions (DAI)

The outlined technological developments suggest that critical cooperative tasks can now be fully automated while retaining oversight, but without the ability to intervene. On first sight, this suggests the complete codification and delegation of cooperative tasks to the blockchain into a DAO. However, this naïve conception obscures the reality of useful socio-technical systems. As with conventional socio-technical systems, the value of any system is determined by its usefulness to solve a specific, more or less well-defined task. However, the central determinant of usefulness remains the human stakeholder that interacts with the system, or, in extension, employs an artificial entity to interact with the system on one's behalf. Instead of replacing existing structures, the technological developments allow new formal organisational structures to emerge in such a way that it is the software that is at the centre of explicitly specified objective coordination tasks, freeing external entities from economically inefficient and potentially corruptible third-party oversight. We call those **Distributed Autonomous Institutions (DAI)** (see Fig. 3).

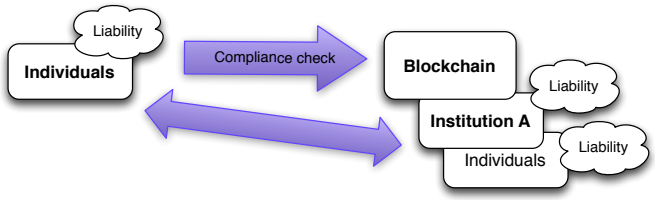

Figure 3. Relationships in Distributed Autonomous Institutions

In DAI the need for trust is eliminated, since the entire workings of the institution (Institution **A** in Fig. 3) are now transparent. The compliance-enforcing role is taken up by individuals. There is no need for a second institution (Institution **B** in Fig. 1) that overlooks workings of Institution **A**. Furthermore, the liability can be partially delegated to individuals.

The software and blockchain technology is capable of providing a transparent, verifiable process to achieve the same effects that traditional organisations achieve with the help of trusted human institutions and governmental services. The essential difference is that DAIs can be made difficult to circumvent and impossible to penetrate. For example, in

 ISBN: 978-1-61208-504-3

economically critical services, such as those offered by banks or governmental agencies, a closed system susceptible to manipulation or fraud can be replaced by a DAI that is more efficient, effective, and which cannot be circumvented by the human element. In contrast to DAOs, the proposed DAI construct includes the consideration of the physical, legal and social environment, as well as contractual relationships residing *outside* the blockchain. This is not meant to reflect a compromise of opportunity and reality, but the merger of the best of two worlds, enabling novel forms of multi-party business-to-business (B2B) operations in which the trust does not need to be mutually negotiated (e.g., relationships between k companies would require $(k(k-1))/2$ contracts) but be attached to an externalised single smart contract accessible and verifiable by either party. This raises enormous potential to construct ad-hoc operations, while providing opportunities to smaller market players that would otherwise not have the capacity to engage in formal negotiations. We specifically want to highlight the explicit formal specification, which, in principle, removes any need for ex-post legal interpretation, since the programmatically encoded agreement is indisputable in legal proceedings, substituting the judicative element necessary for the interpretation of conventional contracts.

The mechanisms discussed above have the potential to fundamentally change the way in which organisations can deal with any form of agreement enforcement, such as individual or collective employment contracts, voting in unions, crowd-funding of startups, or research and development initiatives. However, this notion of verifiable institutions offers novel applications for the revision of the transparent management of funds in governmental organisations, or to facilitate elections. In April 2016, the Minister for the UK Cabinet Office and Paymaster General, Matt Hancock, delivered a speech on Central Government Efficiency, Government Transparency, and Accountability [26], and argued for the use of blockchain technology in the governmental sector:

"We are exploring the use of a blockchain to manage the distribution of grants. Monitoring and controlling the use of grants is incredibly complex. A blockchain, accessible to all the parties involved, might be a better way of solving that problem. [...] Bitcoin proved that distributed ledgers can be used to track currency as it is passed from one entity to another. Where else could we use that? Think about the student loans company tracking money all the way from treasury to a student's bank account. Or the department for international development tracking money all the way to the aid organisation spending the money in country. [...]"

Currently, we are experiencing the dawn of this technology, and we will experience the rise and demise of various blockchain instances, but we can be certain that the technology core is here to stay. Consequently, we will need to observe how it will change the structure of organisations, how we model socio-technical systems, but also what the ethical implications of concepts such as smart self-enforcing institutions are for our disciplines and society.

Inasmuch as we highlighted the benefits of the technology, we consequently need to be aware of the associated risks that follow suit. Will smart contracts and distributed autonomous institutions mimic the existing brick-and-mortar organisational structures, or will we observe new, qualitatively different loosely-coupled socio-technical systems? Can we provide mechanisms that control the advent of novel schemes in which users enter contractual agreements they do not fully understand? Is the lack of case-based control, fraud or manipulation always desirable? Will democratic governments or public companies be expected to adopt transparent and verifiable processes based on the blockchain technology? Can blockchain technology be a solution to facilitate effective and efficient electronic voting? An important aspect in this context is to define how to redraw the line between public and private information (and to implement it). Does this technology prevent novel creative accounting practices (based on improved transparency), or will the low adoption threshold in fact stimulate the emergence of new variants of complex services (e.g., mortgage-backed securities) that have caused economic turbulences in the past? What will the accessibility of smart contracts mean for personal privacy in general?

V. Summary, Discussion & Outlook

Distributed ledgers and distributed consensus protocols replace the need for third party trust. We have argued that the new technology enables the formation of private, anonymity-preserving, yet trustworthy automated institutions. This new flavour of institutions will have characteristics not found in current institutional constellations, due to the nature in which trust and liability are managed. This has the potential to fundamentally change the nature of institutions, because the human element can be eliminated. The blockchain technology allows new forms of governance, liability and trust to be shifted from traditional institutions (such as governments, banks, courts) to individuals and delegated to automated distributed autonomous institutions. The old and the new forms of organisations will co-exist by forming complex structures and interdependencies between human-centric and DAIs. We argued that those new forms of organisational structures are qualitatively distinct from existing institutions. Developing such systems will require a change in how we model systems in general, how we interact with them, but most importantly, how to determine and control the authority we delegate to those systems. This will inevitably involve research and analysis into the impact that DAIs will have on society at large.

To realise the benefits of developing transparent open coordination systems, substantial amount of work is required. Beyond the obvious technical challenges, this requires the consideration of social and legal implications. The potential anonymity enabled by the technology requires careful consideration for applications that may afford some public display of identity-related or pseudonymous information, such as in crowd-funding systems, or land title management. An essential aspect here is to prevent potential defamation by anonymous parties, e.g., by levering a comparable level of identifiability for all involved parties. Those are important design decisions that lie outside the technical platform provided by Ethereum, or blockchain technology more generally, and precede the implementation of a specific contract. An associated problem is the public nature of the blockchain. This implies the awareness that deployed code is and will be publicly accessible, both for inspection but also potential abuse, which lifts the challenge of developing high-quality non-exploitable code, an aspect we discussed in Section III.

Another important aspect revolves around the handling of conflicts. Whenever operating across system boundaries

 ISBN: 978-1-61208-504-3

– such as conventional private organisational environments and publicly-accessible institutions – conflicts can develop and manifest themselves based on changing local operations or environmental influences. The current state of blockchain technology in Ethereum does not consider a dynamic nature of contracts. Once deployed, contracts have a fixed interaction interface and codified operations. This neither considers the potential to adapt contracts at runtime, nor does include mechanisms to mediate conflicts directly. Instead, an alternative refined contract could be negotiated to replace the original contract (that could continue to coexist or simply be discarded). A central consideration in this context is the management of *ownership* of a given contract, i.e., the party/parties that manage/s the life cycle of a given contract. Per default, the instantiating party gains ownership, an aspect that is important for handling of funds that are allocated to a given contract, etc. Unlike conventional contractual agreements, the technically guaranteed executable contract specification affords the explicitly encoding of infrastructural aspects, such as the redistribution of outstanding funds to individuals, the payment of obligations by individual parties to sponsor the contract execution in the first place (i.e., the necessary *gas*), and the necessary actions for discarding a contract (e.g., multi-party invocation of a specified *discard* function).

These interdisciplinary aspects are grounded in technology, but reach far beyond the purely technical domain into management and the legal discipline. This makes it only more important to ensure the safe specification, deployment, and operation of smart contracts. To make smart contracts truly accessible, future development needs to provide mechanisms that allow non-technical users to write prototypical contracts while maintaining the essential institutional content. A possible approach includes the modelling in a widely accessible specification language and the translation into the corresponding execution language in a (semi-)automated manner. An alternative is to provide domain-specific 'building blocks', e.g., for the purpose of 'voting' or 'auctioning', in order to compose executable contracts that could be specified and reviewed by domain experts. An intermediate step would be the specification of best practices and provision of pattern repositories that contain thoroughly tested contracts ready for immediate instantiation.

Further support for developing smart contracts is complemented by the demand to make *existing* smart contracts easily accessible or interpretable to use blockchain technology for its essential purpose: to coordinate verifiable state in a decentralised manner. This would stimulate the broad adoption of this coordination infrastructure by applications and services in a potentially loosely-coupled manner, and extend the playing field beyond the current currency-centric niche existence of blockchain technology.

Bearing the potential and challenges of this novel technology in mind, one thing is certain: Lawrence Lessig captured the essence of DAI, and blockchain technology more generally, when he stated: "code is law" [27].

REFERENCES

[1] G. M. Hodgson, "The Evolution of Institutions: An Agenda for Future Theoretical Research," *Constitutional Political Economy*, vol. 13, no. 2, pp. 111–127, 2002.

[2] L. Bloomfield, *Language*. New York (NY): Holt, 1933.

[3] D. C. North, *Institutions, Institutional Change, and Economic Performance*. New York (NY): Cambridge University Press, 1990.

[4] C. K. Frantz, M. K. Purvis, B. T. R. Savarimuthu, and M. Nowostawski, "Modelling Dynamic Normative Understanding in Agent Societies," *Scalable Computing: Practice and Experience*, vol. 16, no. 4, pp. 355–378, 2015.

[5] W. R. Scott, "Approaching Adulthood: The Maturing of Institutional Theory," *Theory and Society*, vol. 37, no. 5, pp. 427–442, 2008.

[6] D. C. North, "Institutions," *Journal of Economic Perspectives*, vol. 5, no. 1, pp. 97–112, 1991.

[7] I. Stoica, R. Morris, D. Karger, M. F. Kaashoek, and H. Balakrishnan, "Chord: A scalable peer-to-peer lookup service for internet applications," in *SIGCOMM'01*, 2001, pp. 149–160.

[8] C. Dwork and M. Naor, "Pricing via processing or combatting junk mail," in *Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology*, ser. CRYPTO '92. London, UK, UK: Springer-Verlag, 1993, pp. 139–147. [Online]. Available: http://dl.acm.org/citation.cfm?id=646757.705669

[9] QuantumMechanic, "Proof of stake instead of proof of work," https://bitcointalk.org/index.php?topic=27787.0, 2016, accessed on: 1st May 2016.

[10] M. De Oliveira, M. Purvis, S. Cranefield, and M. Nowostawski, "A distributed model for institutions in open multi-agent systems," in *Knowledge-Based Intelligent Information and Engineering Systems*. Springer, 2004, pp. 1172–1178.

[11] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, 2014.

[12] K. Finley, "A $50 million hack just showed that the dao was all too human," http://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/, 2016, accessed on: 1st June 2016.

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

[14] A. M. Antonopoulos, *Mastering Bitcoin: unlocking digital cryptocurrencies*. O'Reilly Media, Inc., 2014.

[15] E. Ostrom, *Governing the Commons: The Evolution of Institutions for Collective Action*. New York (NY): Cambridge University Press, 1990.

[16] E. Smart, "Does china's control over bitcoin mining threaten bitcoin?" http://dcebrief.com/does-chinas-control-over-bitcoin-mining-threaten-bitcoin/, January 2016, accessed on: 1st June 2016.

[17] J. Harrington and G. Caffyn, "Chainalysis network monitoring," http://bit.ly/chainalysis_1, http://bit.ly/chainalysis_2, 2015, accessed on: 1st June 2016.

[18] A. Quenston, "Ethereum reaches unanimous agreement to hardfork," https://www.cryptocoinsnews.com/ethereum-reaches-unanimous-agreement-hardfork/, 2016, accessed on: 10th July 2016.

[19] Bitland, "bitland - land title protection ghana," http://www.bitland.world/, 2016, accessed on: 1st June 2016.

[20] S. Higgins, "Congressional committee hears testimony on blockchain in health care," http://www.coindesk.com/us-think-tank-suggests-blockchain-application-insurance-risk-pooling/, 2016, accessed on: 1st June 2016.

[21] Blockstack, "What is blockstack?" https://blockstack.org/docs/what-is-blockstack, 2016, accessed on: 1st June 2016.

[22] M. Araoz, "Proof of existence," https://proofofexistence.com/, 2015, accessed on: 1st June 2016.

[23] Ethereum Team, "Solidity," http://solidity.readthedocs.io/en/latest/, 2016, accessed on: 1st May 2016.

[24] NXT, "Announcing nxt 2.0!" http://nxt.org/roadmap/, 2016, accessed on: 1st June 2016.

[25] m88888m, "Ethereum with a constitution and legislative initiatives can become a true democracy. while bitcoin still lingers in a plutocratic civil war," https://www.reddit.com/r/ethereum/comments/4qhpo1/ethereum_with_a_constitution_and_legislative/, 2016, accessed on: 10th July 2016.

[26] M. Hancock, "Digital transformation in government and blockchain technology," https://www.gov.uk/government/speeches/digital-transformation-in-government-and-blockchain-technology, April 2016, accessed on: 1st June 2016.

[27] L. Lessig, *Code and Other Laws of Cyberspace*. New York (NY): Basic Books, 1999.

 ISBN: 978-1-61208-504-3