LEDGER
ledgerjournal.org

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2019.178

PROCEEDINGS ARTICLE

A Blockchain Enhanced Framework for Social Networking

Renita M. Murimi*†

Abstract. Social networking sites have given users unprecedented opportunities for the generation and dissemination of content. A variety of social networking sites exist for different purposes, to afford users a range of anonymous and non-anonymous options for self-expression, and the ability to be a part of a virtual community. These "affordances" enable users to create and share content;[1,2] however, the ability to partially or wholly detach user identity from the content has resulted in unique challenges for content access and content attribution. This paper proposes a framework for secure, trustworthy social networking that also creates value for user-generated content by using a blockchain-enhanced framework for social networking. This work explains the application of such a framework for collocated spaces of robots and IoT devices and identifies key challenges that result as a consequence of merging social networking sites and blockchain technology.

1. Introduction

Sharing is a fundamental human experience, and the rise and spread of social networking sites (SNSs) has served to open unprecedented avenues for achieving this experience. Sharing in SNSs has been widely studied, focusing on the causes and consequences of this widespread phenomenon where users have shared both mundane and salient aspects of their lives with online audiences.[3] Recent statistics show that 30% of all time spent online is on social media, with teens leading the pack by spending an estimated nine hours online each day.[4] The increasing amount of time spent online on social media creates new opportunities for marketing research and political campaigns, while also yielding valuable insights into the online and offline lives of users. Content on social media has often been satirized for the breadth of revealed content, ranging from everyday life occurrences such as meals, fitness, personal thoughts and family stories, workplace milestones and challenges, to broader calls for prayers, funds, recommendations, and sharing of news. While serving as fodder for critics of excessive sharing on social media, such content may be viewed in the wider context of a shared life, albeit, one in an online community. Thus, these thoughts and posts are part of the psychology of life stories, ones that long to be told irrespective of the medium, whether it be in under the trees and night skies of ancient societies, in classrooms, in books, or on social media.

The proliferation of social media users and the ability to share content in a decentralized manner has led to significant opportunities for content-creation and monetization. At the same

* 39qEi1VYWbf974oyiZhjWfgk1p2345fssR
† R. M. Murimi (renita.murimi@okbu.edu) is Associate Professor of Computer Science at Oklahoma Baptist University.

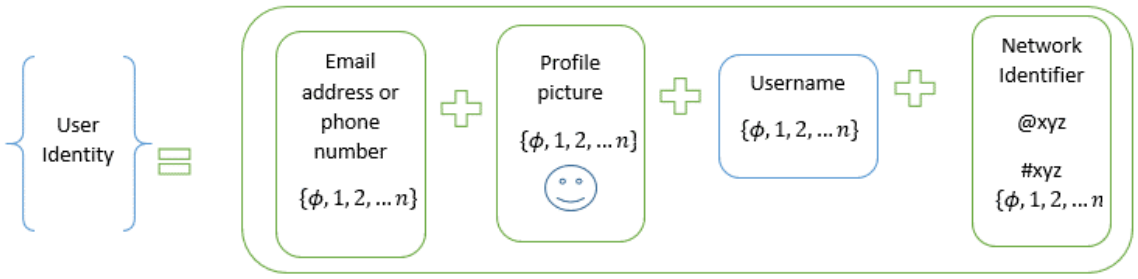

Fig. 1. Components of user identity in online social networks.

time the dissemination of user-generated content on SNSs has also enabled phenomenon such as viral articles, fake news, trolling, and various other cybersecurity challenges that are facilitated by the reach and network design of SNSs. However, existing SNSs do not enable the bulk of social media users to control the reach or monetization of their content.

In this paper, we propose a framework for the blockchain-enhanced version (BEV) of social networking sites. BEV-SNSs leverage the inherent capabilities of blockchain technology to transform the use of SNSs by providing users with control over their sharing preferences and incentivizing their behavior on SNSs.[5] In most existing SNSs, users lack both (a) meaningful control over privacy and (b) value for content. Our framework seeks to achieve both control and value by using blockchain-enhanced versions of SNSs.

2. Digital Identity, Ownership and Monetization

A significant aspect of monetization lies in the challenge of determining digital identity. The artifacts that define a user's digital identity depend on two broad factors - (a) network affordances for identity extraction and management, and (b) a user's willingness for self-disclosure. On non-anonymous networks (*e.g.* Facebook), network affordances for identity extraction and management come in various forms: the use of a profile picture, an option to choose a username, the use of email addresses/phone numbers, and network-specific mechanisms to identify users (*e.g.* the addressing "at" sign @ or the metadata-signalling "hashtag" # in SNSs). On anonymous networks (*e.g.* Whispr), user identity is minimally ascertained due to the absence of or more of the above affordances. However, user willingness to reveal information is equally significant. A user on a non-anonymous network can choose to provide none of the artifacts required for identity extraction. Figure 1 identifies the various components that form a user's digital identity. Each of these components is labeled as one belonging to an infinite set. Thus, a user might create multiple accounts with multiple email addresses, profile pictures, and usernames. A user might choose to supply a profile picture of someone or something else, provide a different name, or use an email address that offers no clues about the real identity of the user. Identification of fake profiles is one piece of the larger puzzle into determining user identity for the sake of attribution of data.[6–10] The challenge with digital identity lies in the determination of the source of content and its trajectory of dissemination through the SNS. In other words, how do we determine who wrote/posted/created content first and how did it spread or morph along its way on the Internet?

The question of ownership gets more challenging as we envision a digital space inhabited by human users, bots, and IoT devices, all of which are capable of creating and sharing content.

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2019.178

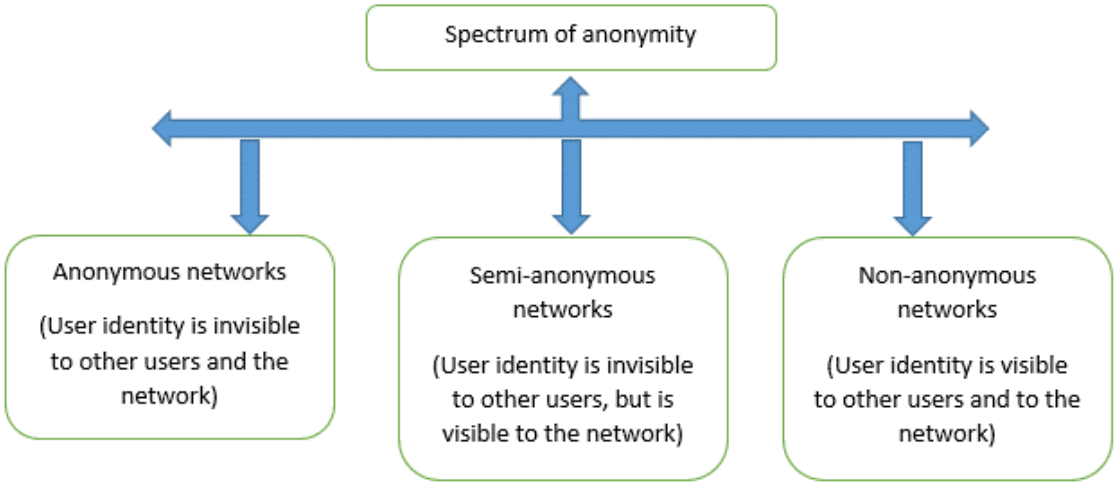

Fig. 2. Spectrum of anonymity on SNS.

Blockchains offer a unique solution to the question of ownership and attribution, and we propose a framework to transform the everyday task of casual browsing and participating in social media into one that offers value for platform-appropriate user activity, while still allowing the user to maintain control over their privacy.

People's motivations to share on SNSs have been extensively studied.[11,12] Previous work has suggested that self-esteem, privacy and sharing tendency were all linked, where users with high self-esteem were shown to be more private, and thus, less needing of input from other users on SNS platforms.[13] This tendency to intertwine self-esteem with feedback from other SNS users also has implications for user behavior in anonymous SNSs. Investigation of SNSs have shown that differing levels of anonymity exist, thus, the spectrum of anonymity (seen in Figure 2) offers users a menu of different platforms for specific networking needs. On one end of this spectrum of anonymity lie SNSs such as Facebook, where the profile-centric architecture of the platform strongly associates a user's content with their profile. On the other end of the anonymity spectrum lie anonymous networks such as Whispr and YikYak where users can post content without the need for creating a profile. Studies have shown that the online disinhibition effect, where people use the affordance of anonymity to act without inhibition and without consideration of social norms on anonymous networks, leads to creation of content that generally tends to feature more negative sentiment and which would not be appropriate for a non-anonymous network.[14,15] Thus, the level of anonymity afforded by a network plays a significant role when users choose to share content.

3. Related Work

Blockchains have shown tremendous potential to transform the user experience in governance, finance, and health informatics. Previous work makes a case for the use of blockchain technology to create "friendly AI".[16] The adoption of blockchain to create secure models of transaction processing has been proposed, where the author points to the use of blockchain to create an "Internet of value" and proposes a framework for governments to adopt blockchain to build a

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2019.178

global digital economy.[17] The role of governments in moving toward a blockchain-enabled model of governance is addressed, where the authors propose replacing public ledgers in industries such as healthcare, the food supply chain, and real estate, alongside traditional application domains such as banking and finance.[18]

Recent literature surveys have shown the applicability of blockchain to various domains in multi-agent systems.[19] These applications include medical records and clinical studies, digital rights management, and intellectual property rights in innovation.[20–22] The authors of the latter describe the role of blockchains in several open innovation domains focusing on notary services, IP registry, licensing, and record keeping, that leverage the inherent distributed, trust-free transaction-processing and record-keeping properties of blockchains.[22]

Research in Blockchain-enabled robotics systems uses blockchains to provide security in swarm robotics in the presence of Byzantine (faulty or malicious) robots.[23–26] In one case, researchers implemented a blockchain-enabled approach for robots in a task where the goal was to detect the most frequent color on a black and white grid. Their work showed that blockchain-enabled swarm robotics was able to detect and exclude Byzantine robots from contributing to the consensus on the most frequent color in the distributed ledger, thereby barring them from influencing the opinions of peer robots in the swarm.

An Autonomous Intelligent Robot Agent (AIRA) protocol for autonomous systems in a peer-to-peer network using Ethereum was tested for the Drone Employee project, which aimed at creating the infrastructure for unmanned aerial vehicles (UAVs) and their dispatchers.[27] The dispatchers obtained topographic data, prepared a route and placed it in the blockchain, leading to execution of the rote by UAVs using transaction data from the blockchain.

Blockchain-based architecture has also been used for enabling secure, fault-tolerant communication between production components involved in IoT applications.[28]

Work has also been done in developing semantics for connecting robotics systems and blockchain networks.[29,30] An ontological framework for resource interaction in blockchain-enabled heterogeneous robotic networks was deployed on two kinds of robots: measuring robots and manipulating robots in a cargo delivery application.[28] The measuring robot measured the size of an obstacle and relayed this information to the manipulating robot, which decided if it could overcome the obstacle. The blockchain stores information about robots that are available for a task, including robots with appropriate hardware, and robot ratings which are determined from their history of efficient task execution.

RoboChain is a framework that facilitates data sharing by multiple robot units, thereby creating avenues for distributed learning and smart medical interventions, while also preserving data privacy.[24] Data privacy was achieved using OPAL, a novel paradigm where algorithms were "sent" to the nodes containing data, instead of the data being copied from a central repository.[31] Thus, these algorithms/queries were executed at the nodes that contained datasets, and the results of the query execution were sent to the entity requesting data. Using a blockchain, the query and results pair was captured and stored on the distributed ledger in a suitable format.

Blockchains have been used to secure peer-to-peer localized commodity trading, where plug-in hybrid electric vehicles (PHEVs) can locally trade electricity.[32] PHEVs with surplus electricity can trade electricity at parking lots and charging stations, thus creating decentralized smart grid that enabled local transactions, unlike the conventional electricity grid that would require complex transportation. To mitigate concerns about privacy, the work proposed the

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2019.178

use of a consortium blockchain, and enhanced blockchain technology with multiple local node aggregators that shared the distributed ledger.

Further work in the use of blockchain blockchain technology for matching services such as multimedia production, ridesharing, freelance work, digital resumes, and personal fitness has also been surveyed.[33,34]

In the next section, we describe our BEV-SNS framework for securely archiving, monetizing and controlling access to user data on SNSs.

4. System Model

4.1. Proposed Framework—Figure 3 illustrates our proposed framework for the BEV-SNS model. User activities in SNSs are stored in the blockchain, along with queries for the data that are generated by system application programming interfaces (APIs). The blockchain stores information about user content, preferences for sharing, rewards for sharing content, and records about data access. This framework for content generation and incentivization by enabling secure transaction processing and record keeping is illustrated further in Figure 4. There are two components to this framework: the user data, and the enhanced blockchain-based digital ledgers that contain algorithms for selecting sharing and reward-generation mechanisms.

- Level 1: Raw data archive: User-generated data (raw data) is the original dataset containing all transactions performed in a network. We define transactions as the set of actions performed on various websites. For example, on a non-anonymous social network such as Facebook or LinkedIn, transactions include account creation, logging in, access to other user's profiles, posts, shares, file uploads and downloads, and the use of network affordances to facilitate communication. Similarly, on an anonymous network or website, transaction performed by a user include writing comments on blogs, editorials, anonymous forums or chat spaces, and the use of other anonymous network affordances. Thus, content generated by a user on various kinds of social networks is created, updated and stored in the raw data archive in the blockchain. In addition to content generated exclusively by the user, SNSs and many websites offer users the ability to "share" data with their networks. This data is generated by other users on the network and sometimes shows up as recommendations on the users' feeds. The raw data archive contains a log of such content that the user accesses from other network APIs and users, thus creating a comprehensive log of all activities performed by the user on a range of websites and networks.
- Level 2: Sharing algorithms: The user can choose the sharing preferences for her data. Thus, sharing preferences are not just dictated by the network or website settings on privacy and sharing. By tuning the disclosure preferences on these algorithms, the user can control the subset of her friends on a SNS that can access her data and can choose what portion of her anonymous data is available for access by other users on various platforms. A user's shared data is a subset of her raw data and is stored in the shared data archive in the blockchain.
- Level 3: Reward algorithms: Content creation, attribution, and licensing can be enabled in the BEV-SNS sharing models. Here, the blockchain stores information about the content and types of data accessed by third-party APIs and other users. Since data is now

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2019.178

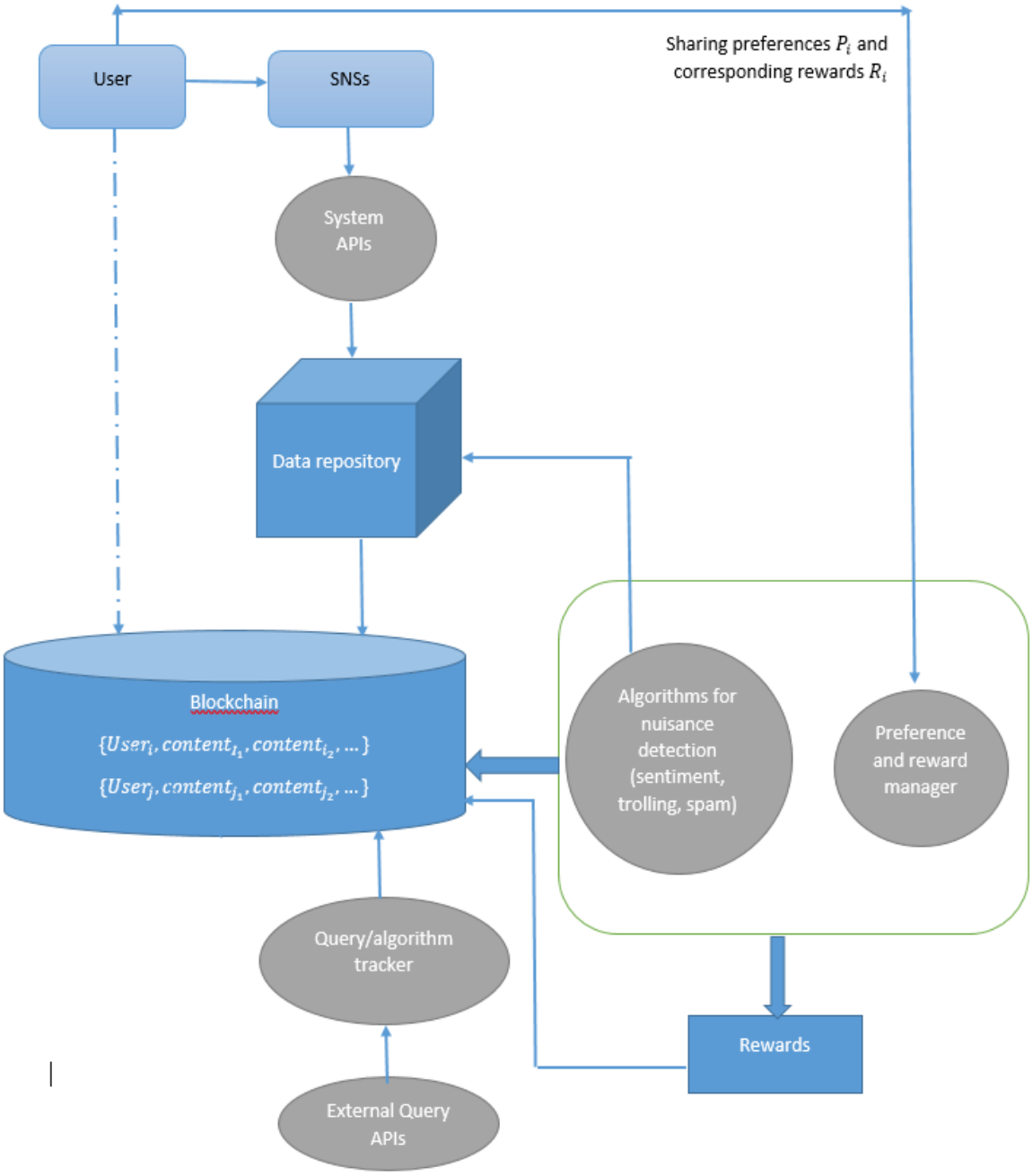

Fig. 3. System architecture and data model for BEV-SNS.

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2019.178

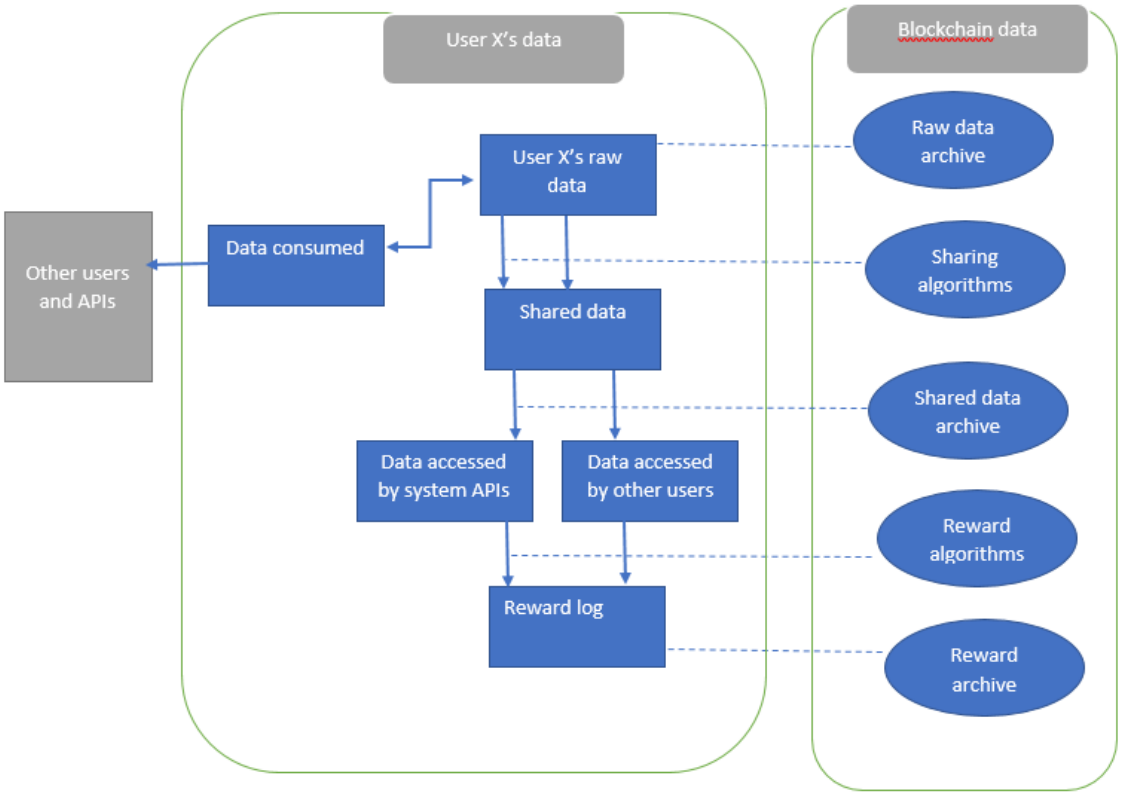

Fig. 4. System model and data flow.

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2019.178

associated with control mechanisms to share the extent and frequency of access by other users, this framework enables monetization of data, creating an Internet of value out of online networking transactions, that have been hitherto viewed as casual, time-zapping activities.[30] Using AI/ML algorithms, the reward mechanisms can be constructed to "learn" sharing preferences and diversify network feeds to avoid homogeneous sources of shared information.[35] This also gives the user greater control over her data access, ensuring that the content she creates is made available to others as per the privacy parameters in her blockchain node.

- Reward archive: Since this framework is capable of data attribution on both anonymous and non-anonymous networks, it can be used to create incentives for content creation and access. This framework has several advantages for both the system and the users, in both anonymous and non-anonymous settings. First, it allows non-anonymous networks such as Facebook better tools for marketing and analytics. Since the origin of user-content can be traced, it can be used to effectively track the number of users that engage with content of various kinds. Users can be rewarded for their transactions on the network by choosing the reward algorithms that are suited to their privacy and monetization preferences. These rewards can be in the form of digital tokens and are also stored on the blockchain in the BEV-SNS version, creating a log for the user that enables her to create associations between her online SNS usage, sharing preferences and rewards. Recognizing that certain kinds of content are well-suited for anonymous settings, or that certain content is only for work, or close friends and family, they can choose to limit its visibility and accept a lower payoff through the reward algorithms. Second, it can be used to mitigate the unintended negative impact of network affordances, such as the rapid sharing of viral content promoting shaming or bullying, and the spread of misinformation or "fake news." In BEV-SNS, the trajectory of such viral sharing can be traced and halted by alerting appropriate nodes to deny permissions to share. Finally, this framework can be used to "civilize" the content posted in anonymous settings such as forums, chat spaces and anonymous SNSs. AI/ML-based reward algorithms can vet the content using sentiment-detection algorithms, spam-filtering, and similar other computational mechanisms to ensure that the content is appropriately rewarded. AI/ML algorithms for shared data can also be used to diversify a user's news feed, creating opportunities for heterogeneous sources of news and information, thus mitigating the effect of homophily and the creation of "echo chambers." The attribution of data, along with associated rewards for forum-appropriate behavior, can limit the kinds of behavior induced by the lack of inhibition in anonymous settings and create incentives for more responsible behavior online.

4.2. Collocated Spaces—Figure 5 shows the framework for collocated spaces of humans and bots communicating with each other through a BEV-SNS wrapper. The blockchain wrapper is an extension of the framework described above, which contains several layers of algorithmic vetting of sharing preferences and content-generation. Several scenarios are envisioned:

- Conventional SNSs: The current use of SNSs is primarily viewed as a means to connect with other users, to conduct meaningful transactions in a manner that mimics offline social norms, and to discover new sources of information. BEV-SNSs are capable of supporting all of these features, while adding reliable records of transactions and creating ways for users to limit access to their data and generate value.

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2019.178

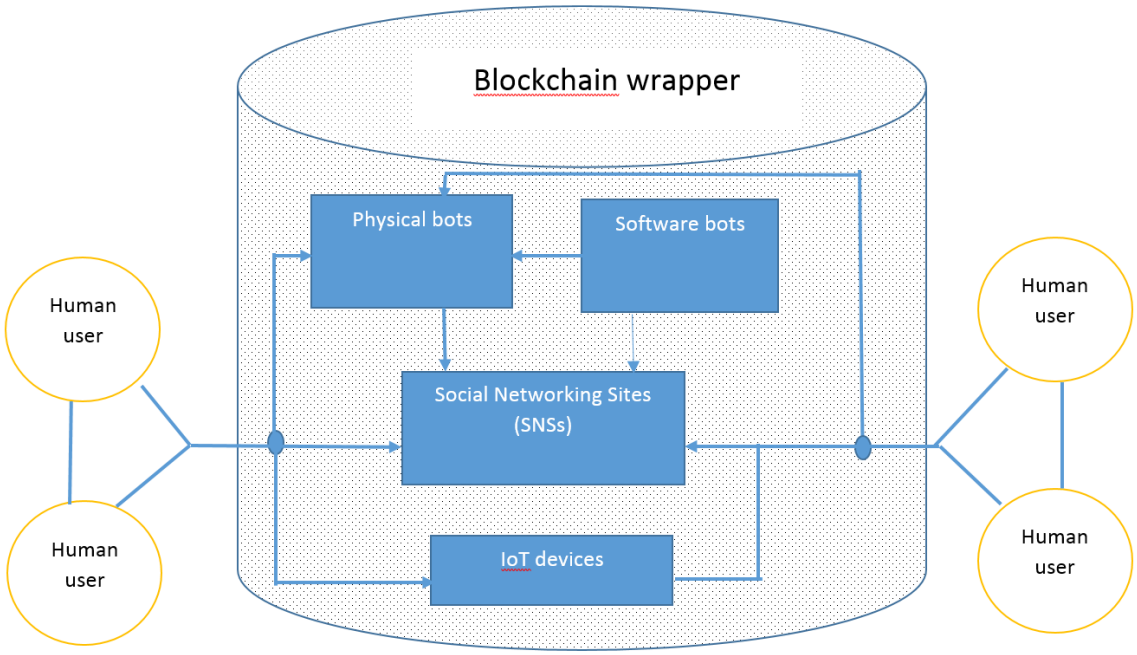

Fig. 5. Collocated spaces of humans, Iot devices and robots.

- Humans and bots: As more and more assistive robots are making their way into our environments, it is envisioned that these robots might be capable of communicating with each other and with humans. Grabbing a coffee with a friend and a robot might not seem far-fetched, and similarly a vacuuming robot having its own SNS profile and accessing it like a human user might be a reality. BEV-SNSs enables a secure environment for different kinds of entities to coexist, while maintaining a uniform model for secure content creation, storage, access, and reward-generation.
- Humans, bots and IoT devices: BEV-SNSs allows for humans, robots and IoT devices to communicate with each other. A smart fridge, smart home-comfort systems and smart car might be capable of interacting with humans and robots (*e.g.* a robot that rides a self-driving car to visit a human).
- Software bots: Recent studies show that software bots are increasingly utilized for online conversations in applications such as customer service, counselling, sales spambots, content-editing bots, and search-engine crawling.[36] While providing several desirable features such as reduction in customer service response time, automatic detection, and filtering, these have also been shown to create fake identities, called sybils, that can be used to increase follower count, populate user-feeds and generate comments and responses. BEV-SNSs can detect the creation of multiple accounts, and the rewards algorithms can prorate rewards for SNS-specific behavior based on the content generated by the bots. Regardless of the anonymity affordances of the SNS, BEV-SNSs can keep track of content, frequency, and access, while creating a trusted environment for humans and software bots in collocated spaces.

4.3. Global hubs—Figure 6 shows the distribution of global hubs that serve to aggregate data in a clustering mechanism for the BEV-SNS framework. Groups of blockchain nodes form

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2019.178

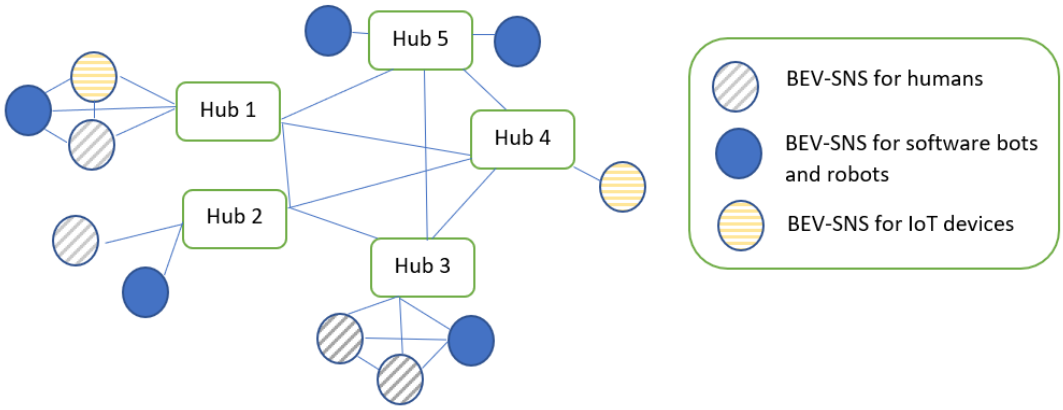

Fig. 6. Global hubs and cluster-heads in BEV-SNS.

clusters and report to a local cluster-head, which is responsible for aggregating data in its cluster, receiving updates and storing data, and connecting to other cluster-heads. The cluster-head performs additional computations to collect, update, store and communicate data with its own nodes and with other cluster-heads. This kind of system model with cluster-heads and groups of individual nodes is found in wireless sensor networks (WSNs),[37] however, it differs from WSNs in that, the nodes in WSNs have their own coverage area for sensing and transmitting/receiving capabilities, which in turn are limited by battery power for sensing and transceiver functions. This causes issues in redundancy, node lifetime and throughput in WSNs. The nodes in the BEV-SNS on the other hand, are not limited by battery power and sensing/transmitting/receiving functions of the on-board processor, and therefore, clusters of nodes are free of challenges in redundancy, optimizing node and network lifetimes, and efficient routing paths. The inherent topology of blockchains leverages redundancy of records to achieve rapid unanimity on deciding legitimate transactions, and inter-node communication is facilitated using lists of IP addresses running as nodes. Since individual user transactions are secured in the blockchain, information about usage patterns, network updates, and maintenance functions can be propagated first to the cluster-heads and then downward in the hierarchy to individual nodes. This distributed model reduces network-wide broadcast communications and mitigates the need for keeping centralized records. Aggregate data at cluster-heads can be parsed for obtaining information about meta characteristics of user interactions on SNSs. Inter-cluster communication between nodes in different clusters occurs via the cluster-heads, thus enabling communications even on sparse networks.

5. Limitations and Challenges

The proposed BEV-SNS framework seeks to incentivize user transactions on SNSs by providing a reward for content-generation, allowing users to choose sharing preferences and keeping secure logs of all SNS activities. For the modern user of SNSs—who values privacy, yet is intentionally or unintentionally revealing a lot of personal information to her networks—a framework where users retain control over their data access and are rewarded for appropriate behavior can create

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2019.178

digital "nudges" influencing their perspective of SNS usage.[38] However, these nudges have several limitations, as we outline below.

- Blockchain limitations: The generation of cryptocurrency has implications for other resources such as the electricity used to mine rewards, the size of the reward, the time required to mine a reward and the scaling of the network to include large-scale SNSs. It is important to create a robust architecture for BEV-SNSs, where the number of SNS transactions to be stored in the blockchain is high.
- Engineering emotions and socially-normative behavior for rewards: It has been shown that anonymous networks favor a lack of inhibition about social norms, thereby causing users to post more intimate content, content that is more negative in sentiment, and content generally of a form that would not be acceptable in a non-anonymous network. Users might also be encouraged to "speak their mind" in an anonymous setting. The design of reward algorithms to incentivize platform-appropriate behavior in BEV-SNSs should be careful to not penalize contradictory sentiment that has valid reasoning, while still being able to detect malicious behavior. This can have significant implications. On the one hand, users might entirely opt out of the reward algorithms, rendering them useless and reverting to the kind of interaction we see in anonymous current-generation SNSs. On the other hand, users might hold back their impulsive opinions and refrain from engaging in challenging intellectual discourse so as to avoid triggering the penalties in the reward algorithms.
- Malicious software bots that generate data for rewards: The BEV-SNS framework employs vetting algorithms that check user-generated content for algorithmic nuisance, such as spam, trolling, and inappropriate behavior. Using ML and deep learning algorithms, this vetting will be conducted at individual nodes to identify "bad actors" and penalize such behavior using reward algorithms.[39] While this process will identify sources of bad behavior and mitigate their influence, it can also be used to game the system by using software bots that generate network-appropriate content to increase the rewards. For example, it might be possible that the ML algorithms sense that posting pictures of early twentieth-century art causes a user's friends to comment on, like, and share these posts more than on her other posts. This also triggers the corresponding reward algorithms to reward such activity more than the user's other activity on the SNS which barely causes any transaction by her network. In such a scenario, it might be that the user employs AI to generate such art frequently in the hope it will generate more rewards. How can such activity be thwarted and what kind of personalized anomaly-detection algorithms would we need? Previous work on sharing preferences has shown that users on SNSs identify themselves as frequent, sparse, moderate sharers or non-sharers (those that merely lurk).[11] Research in anomaly detection systems that extract information about the frequency of posting and the content of a post can help to create a fairer BEV-SNS model.
- Rewards for robots: How can we incentivize good behavior in a robot in an SNS? What is an appropriate reward for a robot in a collocated space? Or should we incentivize only human behavior? AI algorithms employing deep learning and ML are enabling robots to perform activities that are seamless in human environments. A robot that fits right in with humans might be expected to display malicious traits.[40] How can we ensure that we create robot-appropriate nudges? While rewards in the form of bitcoin and other

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2019.178

cryptocurrencies would be native to the BEV-SNS environment and seem appropriate for humans, robots might find little value in these rewards. Substantial research conducted in the area of ethics in a technological society can help to better inform policies and innovation for dealing with collocated spaces of robots and humans as we develop tools to deal with a robot–human society. The implications of data and law can be inferred from Jack Balkin's lecture, in which he proposed laws of robotics for an "algorithmic society."[41,42] The author argues that as algorithms come to the forefront, numerous consequences might be left poorly analyzed without the presence of a broad, regulatory framework that addresses issues of accountability. For example, what are the robot and AI equivalents of punishment for fraud or bodily harm? Issues concerning intent and meaning, as well as monitoring and accountability practices for bots need to be developed that are counterproductive to online nuisances such as hate speech, trolling, and spam, and prioritize trust and value for users of SNSs.

6. Conclusions and Directions for Future Work

In this paper, we proposed BEV-SNS, a framework for incentivizing user behavior on SNSs to achieve two objectives: control over data access, and creation of value through SNS transactions. While the current model of social networking does not offer much in terms of privacy, security, and trust, the inherent architecture of blockchains ensures that the user can tweak the parameters of sharing and rewards in BEV-SNS frameworks for a secure, trusted, and rewarding networking experience. To illustrate this framework, we provided examples of its use with SNSs that lie along the spectrum of anonymity and showed that the framework could be scaled for future use in a variety of collocated spaces. The work in this paper offers multiple avenues for exploring new research areas in computational social science in the age of blockchain technology. This includes the fundamental questions of identifying why people share, and studying whether social norms in offline networking still hold true in SNSs. For example, are "likes" and "shares" motivated not only by content, but also by previous reciprocal transactions? For future work in this direction, we are investigating the nature and design of digital emotions and their expression in SNSs. The design of ML algorithms to better understand sharing preferences and reward mechanisms on various kinds of SNSs are areas of potential research.

Notes and References

[1] Murimi, R. "Online Social Networks for Meaningful Social Reform." In *2018 World Engineering Education Forum - Global Engineering Deans Council (WEEF-GEDC)* (2018) https://doi.org/10.1109/WEEF-GEDC.2018.8629713.

[2] For more on the theory of affordances, see: Gibson, J. J. *The Ecological Approach to Visual Perception*. Psychology Press (2004), especially the chapter entitled, "The Theory of Affordances".

[3] McAdams, D. P. "The Psychology of Life Stories." *Review of General Psychology* **5.2** 100–122 (2001) https://doi.org/10.1037//1089-2680.5.2.100.

[4] Asano, E. "How Much Time Do People Spend on Social Media?" (accessed 16 November 2018) https://www.socialmediatoday.com/marketing/how-much-time-do-people-spend-social-media-infographic.

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

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2019.178

[6] Adikari, S., Dutta, K. "Identifying Fake Profiles in LinkedIn." In *PACIS 2014 Proceedings* 278 (2014) https://aisel.aisnet.org/pacis2014/278.

[7] Conti, M., Poovendran, R., Secchiero, M. "Fakebook: Detecting Fake Profiles in Online Social Networks." In *Proceedings of the 2012 International Conference on Advances in Social Networks Analysis and Mining (ASONAM)* 1071–1078 (2012) https://doi.org/10.1109/ASONAM.2012.185.

[8] De Cristofaro, E., Friedman, A., Jourjon, G., Kaafar, M., Shafiq, M. "Paying for Likes? Understanding Facebook-like Fraud Using Honeypots." In *Proceedings of the 2014 Conference on Internet Measurement Conference* 129–136 (2014) http://dx.doi.org/10.1145/2663716.2663729.

[9] Fire, M., Katz, G., Elovici, Y. "Strangers Intrusion Detection-detecting Spammers and Fake Profiles in Social Networks Based on Topology Anomalies." *Human Journal* **1.1** 26–39 (2012).

[10] Gujarala, S., White, J., Hudson, B., Matthews, J. "Fake Twitter Accounts: Profile Characteristics Obtained Using an Activity-based Pattern Detection Approach." In *Proceedings of the 2015 International Conference on Social Media and Society* (2015) https://doi.org/10.1145/2789187.2789206.

[11] Murimi, R. "On Sharing Preferences in Social Networks." In *Proceedings of the 49th Annual Meeting of the Decision Sciences Institute* 1121–1131 (2018) https://decisionsciences.org/wp-content/uploads/2019/02/dsi-2018-proceedings.pdf.

[12] Morris, M. R., Teevan, J., Panovich, K. "What Do People Ask Their Social Networks, And Why? A Survey Study of Status Message Q&A Behavior." In *Proceedings of the SIGCHI Conference on Human factors in Computing Systems* 39–48 (2010) https://doi.org/10.1145/1753326.1753587.

[13] Christofides, E., Muise, A., Desmarais, S. "Information Disclosure and Control on Facebook: Are They Two Sides of the Same Coin Or Two Different Processes?" *Cyberpsychology and Behavior* **12.3** 341–345 (2009) https://doi.org/10.1089/cpb.2008.0226..

[14] Suler, J. "The Online Disinhibition Effect." *Cyberpsychology and Behavior* **7.3** 321–326 (2004) https://doi.org/10.1089/1094931041291295.

[15] Zhang, K., Kizilcec, R. F. "Anonymity in Social Media: Effects of Content Controversiality and Social Endorsement on Sharing Behavior." In *Proceedings of the International Conference on Weblogs and Social Media* 0–1 (2014) https://www.aaai.org/ocs/index.php/ICWSM/ICWSM14/paper/view/8077.

[16] Swan, M. "Blockchain Thinking: The Brain as a Decentralized Autonomous Corporation." *IEEE Technology and Society Magazine* **34** 41–52 (2015) https://doi.org/10.1109/MTS.2015.2494358.

[17] Maupin, J. "The G20 Countries Should Engage with Blockchain Technologies to Build An Inclusive, Transparent, and Accountable Digital Economy For All." *Economics Discussion Papers* https://www.g20-insights.org/policy_briefs/g20-countries-engage-blockchain-technologies-build-inclusive-transparent-accountable-digital-economy/.

[18] Hughes, E., Graham, L., Rowley, L., Lowe, R. "Unlocking Blockchain: Embracing New Technologies to Drive Efficiency and Empower the Citizen." *The Journal of the British Banking Association* **5** http://dx.doi.org/10.31585/jbba-1-2-(1)2018.

[19] Calvaresi, D., Dubovitskaya, A., Calbimonte, J., Taveter, K., Schumacher, M. "Multi-Agent Systems and Blockchain: Results from a Systematic Literature Review." In A. Demazeau, B. An, J. Bajo, A. Fernández-Caballero (Eds.), *Proceedings of the International Conference on Practical Applications of Agents and Multi-Agent Systems* Springer 110–126 (2018) https://doi.org/10.1007/978-3-319-94580-4_9.

[20] Daniel, J., Sargolzaei, A., Abdelghani, M., Sargolzaei, S., B., A. "Blockchain Technology, Cognitive Computing, and Healthcare Innovations." *Journal of Advances in Information Technology* **8.3** 194–198 (2017) https://doi.org/10.12720/jait.8.3.194-198.

[21] Huckle, S., Bhattacharya, R., White, M., Beloff, N. "Internet of Things, Blockchain and Shared Economy Applications." *Procedia Computer Science* **98** 461–466 (2016) https://doi.org/10.1016/j.procs.2016.09.074.

[22] deLaRosa, J., *et al.* "A Survey of Blockchain Technologies for Open Innovation." In *Proceedings of the 4th Annual World Open Innovation Conference* 14–15 (2017) .

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2019.178

[23] Castelló Ferrer, E. "The Blockchain: A New Framework for Robotic Swarm Systems." In *Proceedings of the Future Technologies Conference (FTC) 2018* Cham: Springer 1037–1058 (2018) https://dx.doi.org/10.1007/978-3-030-02683-7_77.

[24] Castelló Ferrer, E., Rudovic, O., Hardjono, T., Pentland, A. "RoboChain: A Secure Data-Sharing Framework for Human-Robot Interaction." *arXiv* (2018) (accessed 9 March 2019) http://arxiv.org/abs/1802.04480.

[25] Strobel, V., Dorigo, M. "Blockchain Technology for Robot Swarms: A Shared Knowledge and Reputation Management System for Collective Estimation." *IRIDIA Technical Report Series TR/IRIDIA/2018-009* (2018) (accessd 9 March 2019) http://iridia.ulb.ac.be/IridiaTrSeries/link/IridiaTr2018-009.pdf.

[26] Strobel, V., Castelló Ferrer, E., Dorigo, M. "Managing Byzantine Robots via Blockchain Technology in a Swarm Robotics Collective Decision Making Scenario." In *AAMAS '18 Proceedings of the 17th International Conference on Autonomous Agents and MultiAgent Systems* Richland: International Foundation for Autonomous Agents and Multiagent Systems 541–549 (2018) https://dl.acm.org/citation.cfm?id=3237464.

[27] Kapitonov, A., Lonshakov, S., Krupenkin, A., Berman, I. "Blockchain-Based Protocol of Autonomous Business Activity for Multi-Agent Systems Consisting of UAVs." In *2017 Workshop on Research, Education and Development of Unmanned Aerial Systems (RED-UAS)* 84–89 (2017) https://doi.org/10.1109/RED-UAS.2017.8101648.

[28] Teslya, N., Ryabchikov, I. "Blockchain-Based Platform Architecture for Industrial IoT." In *Proceedings of the 21st Conference of Open Innovations Association (FRUCT)* 321–329 (2017) https://doi.org/10.23919/FRUCT.2017.8250199.

[29] Kashevnik, A., Teslya, N. "Blockchain-oriented Coalition Formation by CPS Resources: Ontological Approach and Case Study." *Electronics* **7.5** https://doi.org/10.3390/electronics7050066.

[30] Skinner, C. *VALUEWEB: How Fintech Firms are Using Bitcoin, Blockchain and Mobile Technologies to Create the Internet of Value*. Singapore: Marshall Cavendish International (2016).

[31] Pentland, A., Shrier, D., Hardjono, T., Wladawsky-Berger, I. "Towards an Internet of Trusted Data: Input to the Whitehouse Commission on Enhancing National Cybersecurity." In T. Hardjono, A. Pentland, D. Shrier (Eds.), *Trust::Data - A New Framework for Identity and Data Sharing* Visionary Future 21–49 (2016)https://www.nist.gov/sites/default/files/documents/2016/09/16/mit_rfi_response.pdf.

[32] Kang, J., Yu, R., Huang, X., Maharjan, S., Zhang, Y., Hossain, E. "Enabling Localized Peer-to-Peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains." *IEEE Transactions on Industrial Informatics* **13** 3154–64 (2017) https://doi.org/10.1109/TII.2017.2709784.

[33] McEvily, N., *et al.* "An Incentivized Blockchain Enabled Multimedia Ecosystem." (2018) Whitepaper (accessed 9 March 2019) https://cdn.current.us/whitepaper.pdf.

[34] Clancy, T. "Blockchain Matching Platforms: An Innovative Way to Connect with Peers." (accessed 16 November 2018) https://www.ccn.com/blockchain-matching-platforms-an-innovative-way-to-connect-with-peers/.

[35] Leskovec, J., Huttenlocher, D., Kleinberg, J. "Signed Networks in Social Media." In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* 1361–1370 (2010) https://doi.org/10.1145/1753326.1753532.

[36] Folstad, A., Brandtzaeg, P. "Chatbots and The New World of HCI." *Interactions* **24** 38–42 (2017) https://doi.org/10.1145/3085558.

[37] Heinzelman, W., Chandrakasan, A., Balakrishnan, H. "Energy-efficient Communication Protocol for Wireless Microsensor Networks." In *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences* (2000) https://doi.org/10.1109/HICSS.2000.926982.

[38] Weinmann, M., Schneider, C., vom Brocke, J. "Digital Nudging." *Business and Information Systems Engineering* **58** 433–436 (2016) https://doi.org/10.1007/s12599-016-0453-1.

ISSN 2379-5980 (online)
DOI 10.5195/LEDGER.2019.178

[39] Gleicher, N. "Removing Bad Actors from Facebook." (accessed 16 November 2018) https://newsroom.fb.com/news/2018/06/removing-bad-actors-from-facebook/.

[40] Horton, H. "Microsoft Deletes 'Teen Girl' AI After it Became a Hitler-loving Sex Robot Within 24 Hours." *The Telegraph* **24** https://www.telegraph.co.uk/technology/2016/03/24/microsofts-teen-girl-ai-turns-into-a-hitler-loving-sex-robot-wit/.

[41] Pasquale, F. "Toward a Fourth Law of Robotics: Preserving Attribution, Responsibility, and Explainability in an Algorithmic Society." *Ohio St. LJ* **58** http://hdl.handle.net/1811/85768.

[42] Balkin, J. M. "2016 Sidley Austin Distinguished Lecture on Big Data Law and Policy: The Three Laws of Robotics in the Age of Big Data." *Ohio St. LJ* **78** http://hdl.handle.net/1811/85769.

SSN 2379-5980 (online)
DOI 10.5195/LEDGER.2019.178