Utilizing Blockchain Technology in Social Media Bot Identification

Shreya Reddy [1], Lisa Ewen [2], Pankti Patel [2], Prerak Patel [2], Ankit Kundal [2], and Sabah Mohammed [2]

[1]Lakehead University
[2]Affiliation not available

October 30, 2023

Abstract

As bots become more prevalent and smarter in the modern age of the internet, it becomes ever more important that they be identified and removed. Recent research has dictated that machine learning methods are accurate and the gold standard of bot identification on social media. Unfortunately, machine learning models do not come without their negative aspects such as lengthy training times, difficult feature selection, and overwhelming pre-processing tasks. To overcome these difficulties, we are proposing a blockchain framework for bot identification. At the current time, it is unknown how this method will perform, but it serves to prove the existence of an overwhelming gap of research under this area.

Hosted file

`FinalReport_Group1.docx` available at https://authorea.com/users/662167/articles/675564-utilizing-blockchain-technology-in-social-media-bot-identification

Utilizing Blockchain Technology in Social Media Bot Identification

Lisa Ewen
Department of ComputerScience
Lakehead University
Thunder Bay, ON, Canada
lewen@lakeheadu.ca

Pankti Patel
Department of ComputerScience
Lakehead University
Thunder Bay, ON, Canada
ppatel63@lakeheadu.ca

Prerak Patel
Department of ComputerScience
Lakehead University
Thunder Bay, ON, Canada
ppatel74@lakeheadu.ca

Shreya Reddy
Department of ComputerScience
Lakehead University
Thunder Bay, ON, Canada
sreddy@lakeheadu.ca

Ankit Kundal
Department of ComputerScience
Lakehead University
Thunder Bay, ON, Canada
akundal@lakeheadu.ca

Sabah Mohammed
Department of Computer Science
Lakehead University
Thunder Bay, Canada
sabah.mohammed@lakeheadu.ca

***Abstract*— As bots become more prevalent and smarter in the modern age of the internet, it becomes ever more important that they be identified and removed. Recent research has dictated that machine learning methods are accurate and the gold standard of bot identification on social media. However, with technology constantly developing, blockchain has become an increasingly powerful framework that has shown promise in the areas of healthcare and finance. At the current time, there is no research exploring the utility of blockchain in a social media bot identification context, and it is important for progression of technology to explore these possibilities. We propose a prototype of a blockchain-based bot identification framework which has the potential to be modified for practical use on modern social media platforms to aid in bridging the gap present between blockchain and bot identification. The prototype is based on the BitCoin system of verification, and has the potential for modifications to be made for further research and an expansion of the conversation surrounding blockchain and social media bot identification.**

Keywords*— *blockchain, smart contracts, bot identification, social media

I. Introduction

While the first bot to be introduced to the Internet, called WebCrawler, was deemed a benevolent bot [4], malicious bots have been on the rise. An area ripe with malicious bots is social media, where the bots not only have a negative impact on the platform, but also on the userbase according to recent literature [7]. In general, social bots tend to be used as fake followers to simulate fame on the platform, participate in spamming, bias public opinion, and limit free speech as determined by Lutz Finger [19], and all actions tend to have significant negative actions to a platform if the bots are allowed to continue existing on the platform. Due to the overwhelming negative effects of social bots, a desire to identify them has emerged in order to remove them from the platform they exist on and prevent them from performing negative actions.

Unfortunately, as often as techniques to identify or thwart bots from infiltrating a website, those who create bots are making them smarter [17]. This results in a never-ending cat-and-mouse game requiring the constant evolution of bot identification techniques. This is prevalent in the evolution of CAPTCHA techniques, beginning as strictly text [16], but eventually involving pictures, audio, and other forms of media to outsmart the constantly-improving bots [18].

Despite the fact that bots are continually learning from the approaches we utilize to identify them, many improvements involve modifying past techniques. An example of this is modifying CAPTCHAs from text to selecting the correct orientation of an image being given [17]. This begs the question: why, instead of improving old methods, do we not develop more unique concepts?

A very powerful concept that was first outlined in 1991 by Habart and Cornetta [2] is blockchain. Originally, it was intended as a method for reliable timestamping, but became popularized in 2008 in a whitepaper by Satoshi Nakomoto where he discussed using blockchain for a cryptocurrency known as Bitcoin [3]. Since its inception, blockchain technology has shown promise in other areas outside of cryptocurrency and other financial applications due to its unique decentralized structure. With the invention of smart contracts, blockchain technology becomes an even more powerful tool that has been shown to have promise in the area of healthcare technology [1, 5, 6].

While CAPTCHA and machine learning techniques have proven to be a popular technique in the field of bot identification, we suggest that an exploration of other frameworks or concepts is necessary to slow down the rate in which social media bots are able to overcome the identification methods. We propose that blockchain-driven framework has many benefits that have yet to be explored in the context of social media bot identification at this time, and that upon further research, it may prove to be a

useful tool against bots. In combination with smart contracts, human involvement, and decentralization, we propose that a forceful bot identification tool utilizing blockchain can be created and eventually utilized in modern social media practice.

II. Related works

As mentioned in the previous section, many of the non-financial applications of a blockchain have been seen in healthcare. This research highlights some of the key advantages of blockchain technology, most notably the immutability and decentralized storage. In the work done by Linn and Koo [8], we see blockchain being used as an access control manager for health records. Despite future research being required to overcome limitations of the approach, this research demonstrates an innovative utilization of blockchain technology which proves that blockchain technology can be utilized in many domains. Similarly, Ekblaw et. al. demonstrated a similar approach by utilizing the fundamental aspects of blockchain to improve EHR systems [9].

Despite the significant work being done to explore the use of blockchain technology in healthcare, the most common methodology in bot detection research utilizes machine learning techniques. An interesting approach by Velayuthem and Tiwari [10] discuss training a model based on Twitter profile attributes (their number of followers, level of completeness, username, etc.) as well as tweeting patterns. A significant aspect of this research, as well as the work done by Alvari et. al. [11], [12], and [13], demonstrates that much of these approaches involve training models to detect patterns among the a given user's public information. While the model architecture chosen, datasets used to train, and features detected by the model are all different, much of the approach is very similar. While all of the models proposed by the aforementioned researches performed well, it is clear that there is a trend among this field of research to train a model based on attributes and activities of a given user using social media.

The current research toward bot identification is primarily focused on machine learning, with some other approaches such as graph-based techniques [14]. At the time of writing, there is no available research on bot (social media or otherwise) identification utilizing a blockchain framework, and thus, there is a significant gap in this line of research. While machine learning and other techniques have proven useful, as mentioned previously, exploration of other methods is extremely important due to the rate at which social media bots are capable of overcoming identification methods.

III. Methodology

Out proposed prototype aims to provide a proof of concept for utilizing blockchain in the context of social media bot identification. It serves to show that it is possible to build such software with the capability of performing bot identification with the blockchain framework, but no formal testing has been done to analyze the scalability, accuracy, or overall feasibility of the proposed prototype.

Due to bot identification with a blockchain framework being an unexplored concept, our main methodology is to provide the conceptual prototype for further experimental trials to fully research the possibilities and potential drawbacks of using blockchain in this way.

The prototype relies on human intuition of a blockchain participant to identify if a given user in the system is a social bot or a human user. This technique is not infallible, obviously, but it does allow users to feel in control of the platform they are a part of should they choose to, and removes a lot of uncertainty that surrounds "algorithms" that typically make the decisions and upset the userbase when misclassifications are made. We have also implemented a ranking system to the prototype to ensure accountability is upheld on those who make errors and dictates to what degree a classification can be trusted based on the participant's ranking. A detailed description of the structure of the system can be seen in figure 1.

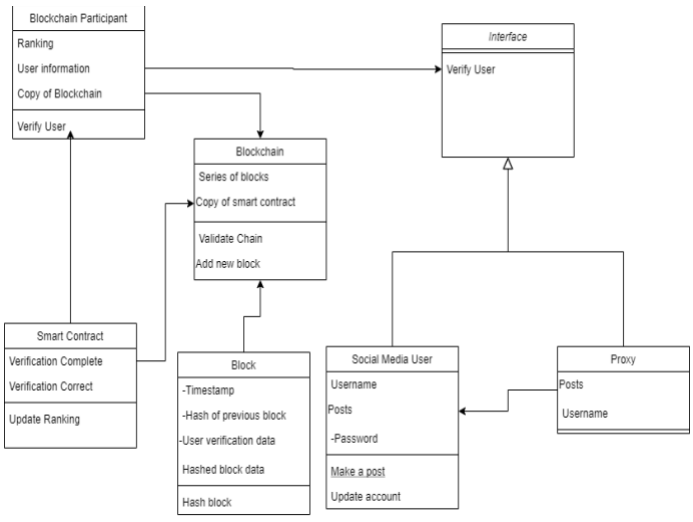

Figure 1. UML Class diagram of the prototype

The main goal of this prototype is to identify bots on a given social media platform (Twitter, Facebook, Instagram, etc.) so that they can be removed. The actual removal of the bots does not take place on the blockchain, however, the responsibility to remove the identified fraudulent users is to be handled

by the platform utilizing the identification platform in whichever means they deem appropriate. The blockchain serves as a ledger accessible to the social media platform to then take action either manually or automatically depending on their system. Examples of use cases for the system are found in figures 2 and 3.

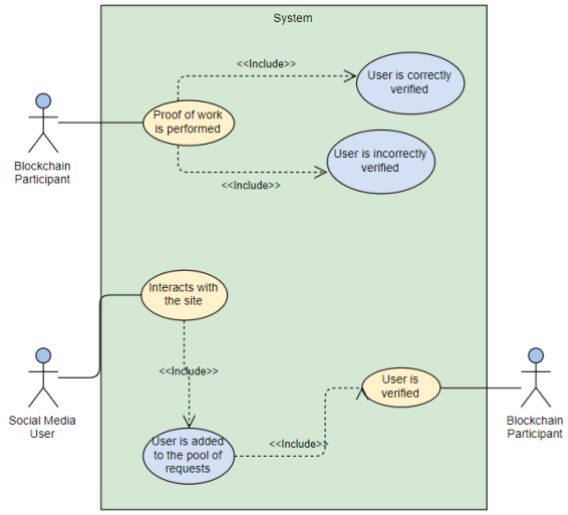

Figure 2. Use cases involving the verification process

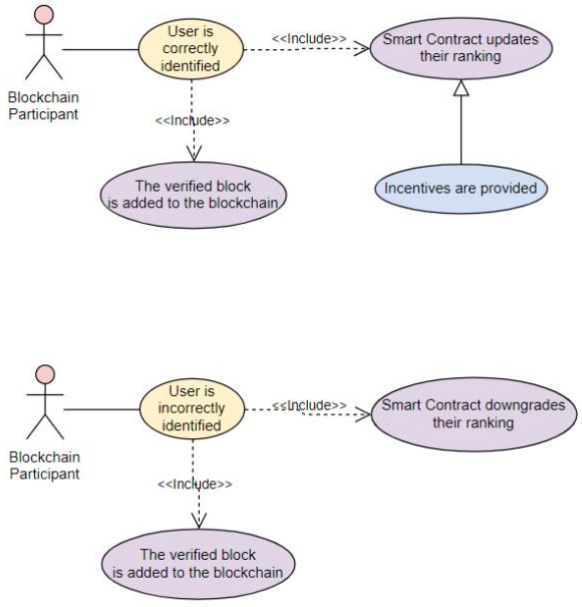

Figure 3. Use cases following the verification process

IV. Prototyping

Our proposed prototype was built with the BitCoin architecture in mind, meaning that the verification of users and/or bots occurs using human involvement. Each participant in the blockchain will view a pool of users and make a determination on whether or not they believe a user is real, or if they are a bot account. Upon making these decisions, the participant is required to perform Proof of Work. For the sake of simplicity in our prototype, we relied on the HashCash Algorithm [15], but different forms of Proof of Work can be implemented in its place during future research. The block diagram in figure 4 explains the process of identification in the prototype.

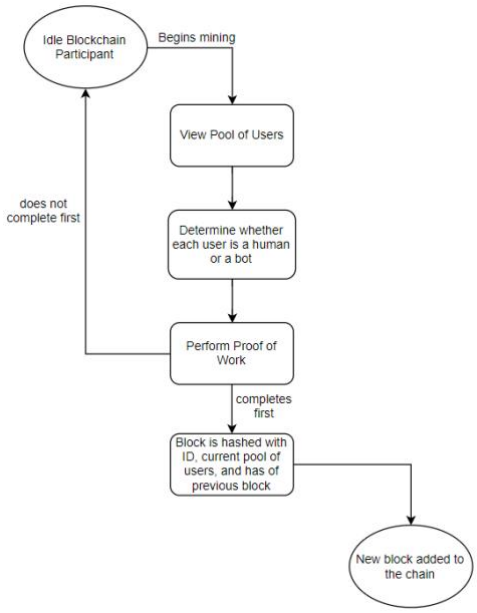

Figure 4. Block diagram of user verification

Our prototype also features a ranking system which is tasked with preventing participants from abusing the system. New participants start with a low rank which increases as they make verifications without incident. Should any verification they make be reported as false, the participant subsequently suffers a degradation in their ranking. Once a participant reaches the lowest ranking, they are removed from the system and are no longer allowed to make verifications.

In order to enforce this rule, a smart contract stored on the blockchain is used. The smart contract is automatically deployed after each verification to increase a participant's ranking, and should any misclassification reports be made, the smart contract will respond accordingly depending on the participant's existing ranking. Figure 5 features pseudocode of the smart contract.

Finally, the prototype features a distributed database design. The blockchain is stored in a single table with a row in the table representing a single block in the blockchain. Each participant of the system has a copy of this database, and therefore, a copy of the blockchain which is updated after each verification made on the system. The database also features all users in the pool of users to be verified, as well as the public information of each participant of the blockchain (i.e.

their public username and their ranking). The ER diagram of the database is seen in figure 6.

Algorithm 1: Smart Contract

Result: Participant's ranking is updated or they are removed

initialization;
if *Verification is complete* **then**
  update participant's rank;
end
if *A verified user was misclassified* **then**
  reduce participant's rank;
  if *Participant's rank is below 1* **then**
    remove participant from the system;
  end
end

Figure 5. Smart contract pseudocode

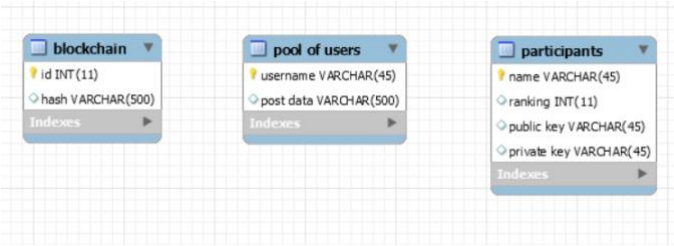

Figure 6. ER Diagram of the database

The discussed prototype is very simple, but has the potential for modification to be used during further exploration of the possibilities of this topic. Possible modifications include, but are not limited to, other proof of work algorithms, implementation of the Proxy Pattern for further security, a more complex ranking system, and a more robust smart contract implementation. Experimenting with these different modifications can expand the potential of the prototype, which can result in significant advancements of this area of research.

We also expect that existing criticisms of other blockchain applications will apply to this prototype as well, such as issues with scalability due to the large distribution of the blockchain, the unnecessary consumption of energy required in completing the Proof of Work, and security issues including DDos attacks, consensus delays, and mempool attacks. Without testing the prototype on a larger scale with significantly more users, it is difficult to know exactly how these issues, or others, may present in order to implement measures to protect against them.

V. Concolusion and Future Work

In the field of social bot identification, it is imperative to quickly develop methods to identify bots, but it is also important to develop methods that may be difficult for the bots to adapt to. Much of the literature on identifying social bots includes CAPTCHA techniques and variations, as well as machine learning methods. While most have very good accuracies, these techniques have much in common with previous techniques, which may make it easier for bots to learn from at a faster pace.

A framework that has been recently popularized, blockchain, is a powerful system that not only has potential to be more difficult for a bot to outsmart, but has other benefits for users as well. This is due to the decentralization, human involvement, consensus, and smart contracts that are a part of the blockchain ecosystem. Our proposed framework makes use of all of these aspects, capable of performing the specified task well at a small scale. Despite this, our prototype serves only as a proof of concept to start a conversation about how best to design a framework of social bot identification using blockchain.

Further research is essential to fully understand the best way to implement this type of framework, as well as the potential benefits and drawbacks. We expect there to be issues pertaining to scalability and the Proof of Work as has been criticized in previous implementations of blockchain in other fields. Without further exploration, it is difficult to know for sure what issues will arise.

Acknowledgment

This paper was written as part of the COMP5112WC course at Lakehead University supervised by Dr. Sabah Mohammed.

References

[1] Suveen Angraal, Harlan M Krumholz, and Wade L Schulz. "Blockchain technology: applications in health care". In: *Circualtion: Cardiovascular Quality and Outcomes* 10.9 (2017), e003800.

[2] Stuart Haber and W Scott Stornetta. "How to timestamp a digital document". In: *Conference on the Theory and Application of Cryptography*. Springer. 1990, pp. 437-455.

[3] Satoshi Nakamoto. *Bitcoin: A peer-to-peer electronic cash system*. Tech. rep. 2008.

[4] Brian Pinkerton. *Webcrawler: Finding what people want.* Citeseer, 2000.

[5] Claude Pirtle and Jesse Ehrenfeld. *Blockchain for healthcare: The next generation of medical records?* 2018.

[6] Kefa Rabah. "Challenges & opportunities for blockchain powered healthcare systems: A review". In: *Mara Res J Med Health Sci* 1.1 (2017), pp. 45-52.

[7] Stella, Massimo, Emilio Ferrara, and Manlio De Domenico. "Bots increase exposure to negative and inflammatory content in online social systems." *Proceedings of the National Academy of Sciences* 115, no. 49 (2018): 12435-12440.

[8] Linn, Laure A., and Martha B. Koo. "Blockchain for health data and its potential use in health it and health care related research." In *ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST*, pp. 1-10. 2016.

[9] Ekblaw, Ariel, Asaph Azaria, John D. Halamka, and Andrew Lippman. "A Case Study for Blockchain in Healthcare:"MedRec" prototype for electronic health records and medical research data." In *Proceedings of IEEE open & big data conference*, vol. 13, p. 13. 2016.

[10] Velayutham, T., and Pradeep Kumar Tiwari. "Bot identification: Helping analysts for right data in twitter." In *2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA)(Fall)*, pp. 1-5. IEEE, 2017.

[11] Alvari, Hamidreza, Elham Shaabani, and Paulo Shakarian. "Early identification of pathogenic social media accounts." In *2018 IEEE International Conference on Intelligence and Security Informatics (ISI)*, pp. 169-174. IEEE, 2018.

[12] Chavoshi, Nikan, Hossein Hamooni, and Abdullah Mueen. "DeBot: Twitter Bot Detection via Warped Correlation." In *ICDM*, pp. 817-822. 2016.

[13] Kudugunta, Sneha, and Emilio Ferrara. "Deep neural networks for bot detection." *Information Sciences* 467 (2018): 312-322.

[14] Nagaraja, Shishir, Prateek Mittal, Chi-Yao Hong, Matthew Caesar, and Nikita Borisov. "BotGrep: Finding P2P Bots with Structured Graph Analysis." In *USENIX security symposium*, vol. 10, pp. 95-110. 2010.

[15] Back, Adam. "Hashcash-a denial of service counter-measure." (2002).

[16] Von Ahn, Luis, Manuel Blum, Nicholas J. Hopper, and John Langford. "CAPTCHA: Using hard AI problems for security." In *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 294-311. Springer, Berlin, Heidelberg, 2003.

[17] Ferrara, Emilio, Onur Varol, Clayton Davis, Filippo Menczer, and Alessandro Flammini. "The rise of social bots." *Communications of the ACM* 59, no. 7 (2016): 96-104.

[18] Singh, Ved Prakash, and Preet Pal. "Survey of different types of CAPTCHA." *International Journal of Computer Science and Information Technologies* 5, no. 2 (2014): 2242-2245.

[19] Finger, Lutz, and Soumitra Dutta. *Ask, measure, learn: using social media analytics to understand and influence customer behavior*. " O'Reilly Media, Inc.", 2014.