International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 06 | June - 2021 ISSN: 2582-3930

Dwitter- Decentralized Twitter using Blockchain Network

Varun Beloria[1], Abhishek Deshpande[2], Harshad Jadhav[3], Prof. Jagruti Wagh[4]

[1234] *Department of Computer Engineering, Marathwada Mitra Mandal's College of Engineering, SPPU, Pune, India*

Abstract - *In today's world social networking platforms such as Instagram, Facebook, Google+ etc, have created the boom in our humanitarian society. Along with these social networking platforms there comes a great responsibility of handling user privacy as well as user data. In most of these websites, data is stored on the centralized system called as the server. The whole system crash down if the server goes down. One of the solutions for this problem is to use a decentralized system. Decentralized applications works on Blockchain. A Blockchain is a group of blocks connected sequentially to each other. The blockchains are designed so that transactions remain immutable i.e. unchanged hence provides security. The data can be distributed and no one can tampered that data. This project presents a decentralized social media like Twitter application which is based on blockchain technology where the user would be able to view, like, comment, share photos shared by different users.*

Key Words:- **decentralized, blockchain, immutable, distributed, tampered .**

1. INTRODUCTION

We believe the solution is a decentralized social network which is encrypted at rest. When the user has the key to decrypt and modify their own data, they have complete control, and can grant and revoke control from third parties. Everyone's data is just 'out there', many copies floating around in encrypted blobs that anyone can host or download but only friends can decrypt. Decentralization also provides robustness against censorship, internet outages, and would-be social monopolies. The key to this decentralized paradigm is not merely security, which is not too hard with public key cryptography, but user friendly security, which lets us have the conveniences we're used to in centralized systems, but keeps the network secure and open to anyone interfacing with it in whatever way they please. We achieve these features, including confidentiality, metadata hiding, profiles, friend networks, instant messaging, groups, and much more through a carefully constructed profile file tree distributed peer to peer. It can be easily updated, distributed via deltas rather than bulk transfers, and hosted without being able to glean any information about that user. Most importantly of all, it lays the foundation for a secure system that people may actually want to use.

In recent years, major social media has been frequently plagued by privacy abuse and data breaches scandals. Facebook has been accused of selling or abusing user data in 2018, leading to identity theft and other related issues.
As a result, Facebook lost over $120 billion in market cap. The event has intensified distrust of centralized OSNs.

In a word, the privacy issues become a major problem that should be resolved for the existing centralized OSNs, which have prompted researchers to consider the decentralization framework for online social networks.

2. MOTIVATION

As you are surely painfully aware, Facebook provides decent service at the extremely high cost of constantly disregarding user privacy, common decency, and laws around the world, and yet they still have billions of users. How can this be possible? They have a monopoly. Monopolies breed complacency, low quality, and high costs. And Facebook has a monopoly over your friend network. You can't leave because everyone is on Facebook. Switching to a new platform means every single one of your friends has to make a new account, download a new app, and you have to rebuild that whole network—if you can convince them at all. It's the same story for any platform (though most don't charge such a high price), and it's unavoidable. Metcalfe's Law states that the value of a network is proportional to the square of the number of its users, so it's no

wonder the network effect is one of the most powerful social phenomena.

3. CONSENSUS

We know that Blockchain is a distributed decentralized network that provides immutability, privacy, security, and transparency. There is no central authority present to validate and verify the transactions, yet every transaction in the Blockchain is considered to be completely secured and verified. This is possible only because of the presence of the consensus protocol which is a core part of any Blockchain network.

A consensus algorithm is a procedure through which all the peers of the Blockchain network reach **a** common agreement about the present state of the distributed ledger. In this way, consensus algorithms achieve reliability in the Blockchain network and establish trust between unknown peers in a distributed computing environment. Essentially, the consensus protocol makes sure that every new block that is added to the Blockchain is the one and only version of the truth that is agreed upon by all the nodes in the Blockchain.

The Blockchain consensus protocol consists of some specific objectives such as coming to an agreement, collaboration, co-operation, equal rights to every node, and mandatory participation of each node in the consensus process. Thus, a consensus algorithm aims at finding a common agreement that is a win for the entire network.

Now, let's see two main consensus algorithms and how they work.

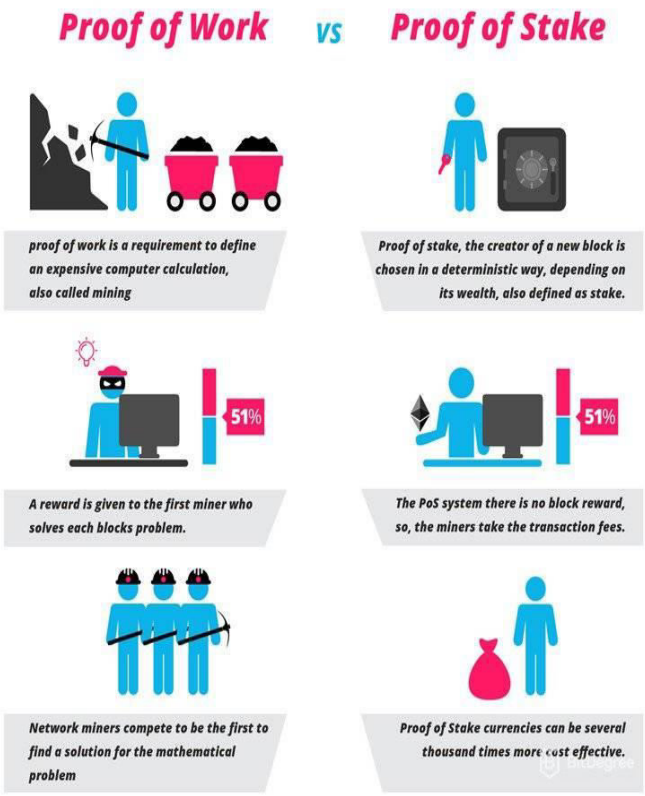
1. Proof of Work (PoW):

This consensus algorithm is used to select a miner for the next block generation. Bitcoin uses this PoW consensus algorithm. The central idea behind this algorithm is to solve a complex mathematical puzzle and easily give out a solution. This mathematical puzzle requires a lot of computational power and thus, the node who solves the puzzle as soon as possible gets to mine the next block.

2. Proof of Stake (PoS):

This is the most common alternative to PoW. Ethereum has shifted from PoW to PoS consensus. In this type of consensus algorithm, instead of investing in expensive hardware to solve a complex puzzle, validators invest in the coins of the system by locking up some of their coins as stake. After that, all the validators will start validating the blocks. Validators will validate blocks by placing a bet on it if they discover a block which they think can be added to the chain. Based on the actual blocks added in the Blockchain, all the validators get a reward proportionate to their bets and their stake increase accordingly.

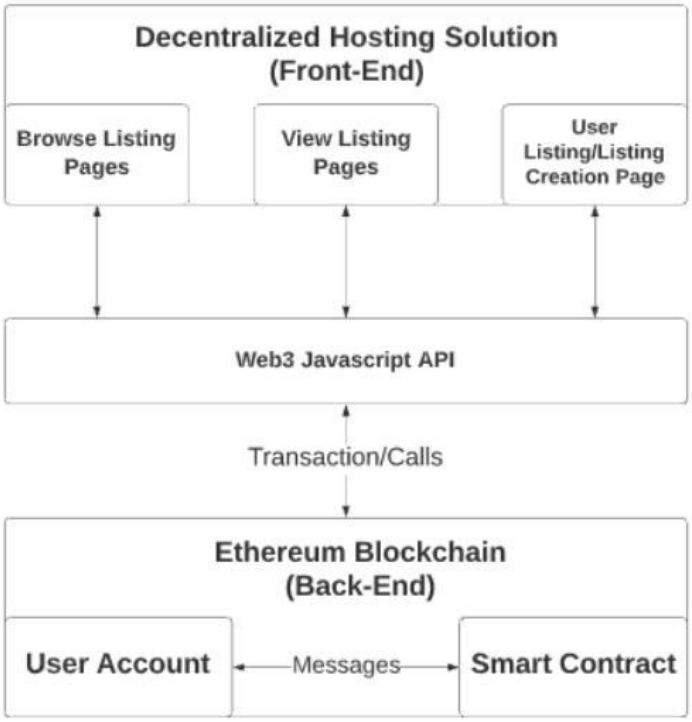
In the end, a validator is chosen to generate



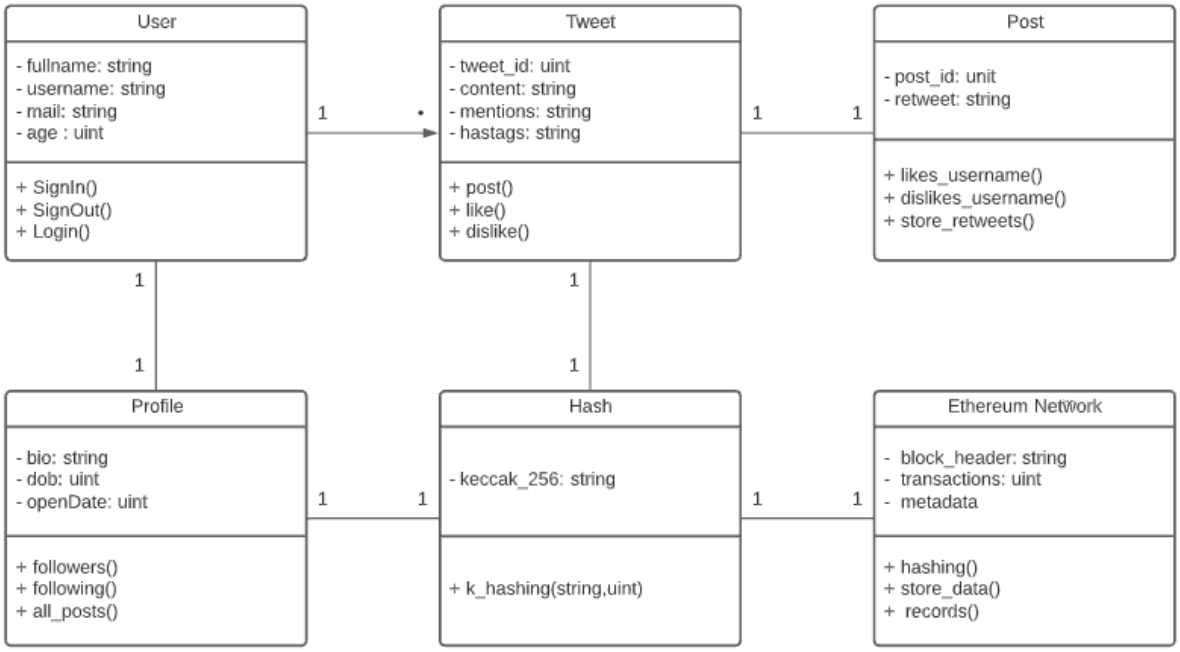
a new block based on their economic stake in the network. Thus, PoS encourages validators through an incentive mechanism to reach to an agreement.

4. FIGURES

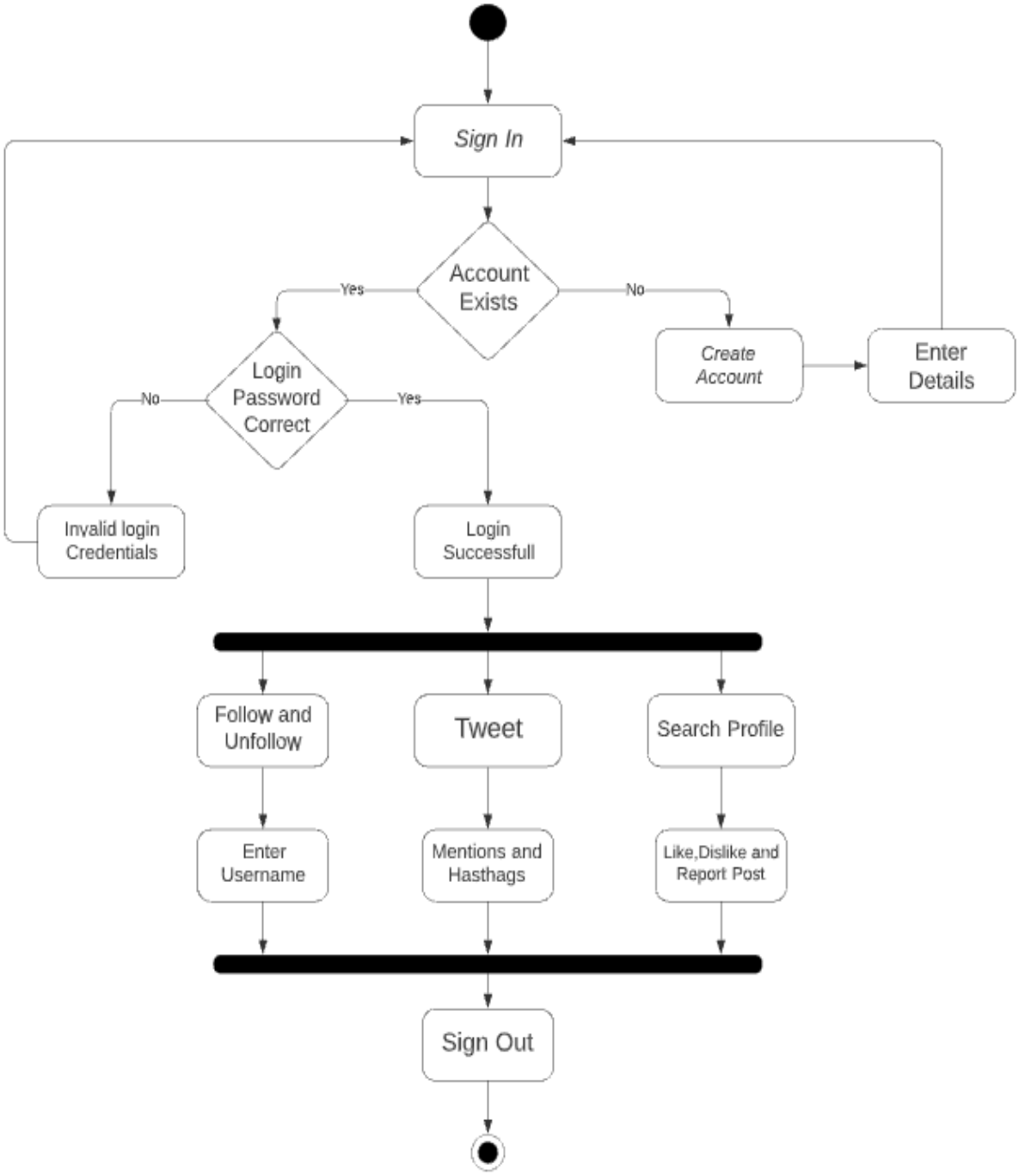
1. System Architecture:



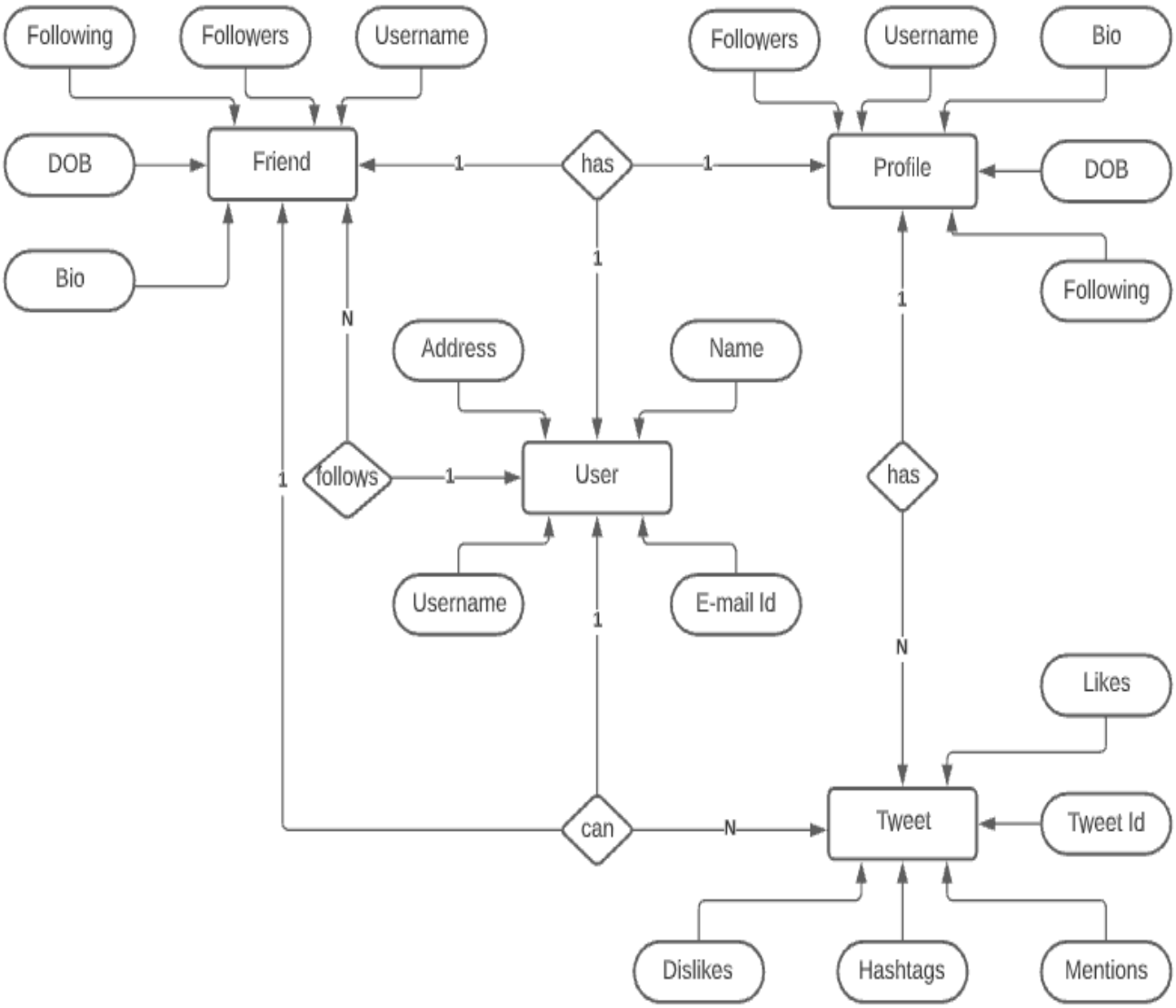
2. UML Class Diagram:



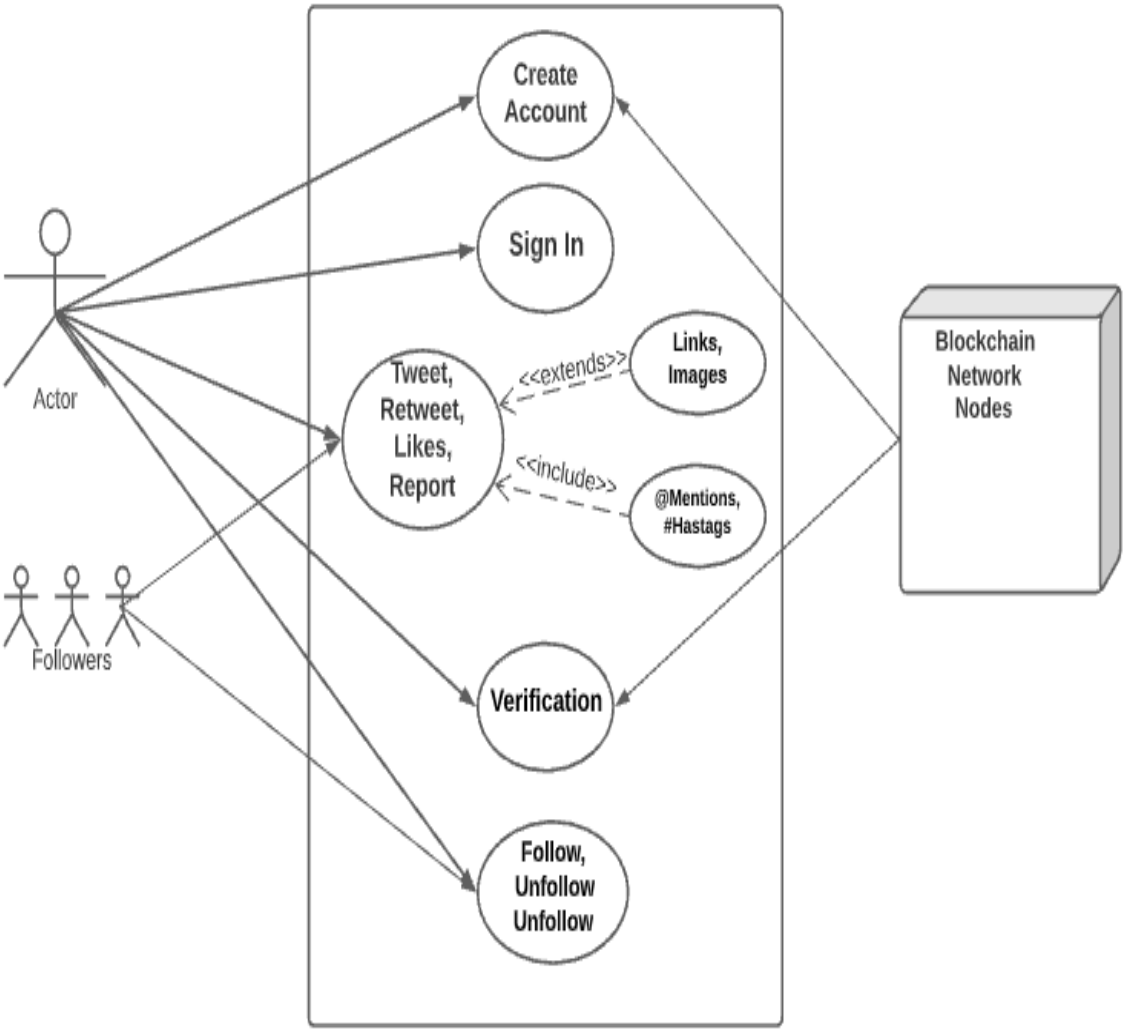
3. Activity Diagram:



4. ER Diagram:



5. Use Case Diagram:



5. PROS AND CONS

Social media promotes connectivity, community building, and knowledge sharing. People can use social media to drive social and political change, bring awareness to important issues, raise funds for those in need, and promote their businesses. However, social media's ugly side can include cyber-bullying, political misinformation, and even criminal activity. Because decentralized social networks are largely un-moderated, both the positive and negative outcomes become more extreme.

User Control, Free Speech and Censorship Resistance:

Corporate entities control major social media sites, and a small group of people within these companies sets the rules of engagement. This has raised concerns about free speech and censorship among users. Banning violent, hateful, and dangerous messaging helps protect social media users from malicious online activity, but some believe the bans run contrary to ideals of free speech. A decentralized social network allows users more control. In other words, users do not accept censorship and insist on having the final say on their content. This means no one else, whether a corporation or site administrator, can make modifications to content created by users.

A downside of this structure is that hate groups also have the freedom to launch their own social media sites. While individuals can block these groups, they cannot prevent them from engaging on the network.

Personal Data, Privacy and Security:

Users own their own data, and companies must hand over more control of personal data to users. Decentralized social networks have provided another answer to data privacy and security. On decentralized social networks, users can create accounts without having to link to real-world identities, like email addresses or phone numbers.

Also these networks often rely on public-key cryptography for account security, rather than relying on a single organization to protect user data.

While this can create advantages from a data security perspective, it also has some downside to it. . For example, bootstrapped federated social networks may shut down because of a lack of funds, causing users to lose their data and connections. In this instance, users have no simple way to reconnect with others on the network because federated networks
do not keep records of personal data on servers.

Economic Neutrality:

Economic neutrality is an essential ideal for many who turn to decentralized social networks — they wish to free themselves from interfering advertising and the risk to privacy it poses. Federated networks look to new forms of monetization to remain solvent. They often use a form of digital currency, such as Bitcoin, to keep operations running.

6. FEATURES:

One of the goals of the system is to achieve a level of privacy while maintaining the same conveniences of a modern social media/group messaging application. The system as described naively supports simple group chats, but more complicated features can be built on top it including admins, read-receipts, custom reacts etc. It is easy to set state and implement arbitrary functionality because the method of sending messages is so general.

Basic Features

- Privacy(e.g Access Control, Metadata-hiding)
- Instant messaging/ Group Chats.
- Read Receipts, Reacts, Mentions and other metadata posts.
- Replies comments/threads/etc .
- Multi device support.
- Sign-in with username/password.
- Nested group.

CONCLUSION:

Online Social networking sites are extremely popular. Those sites provide the means for many Web users to maintain contacts, communicate and exchange information with each other. While existing social networking sites offer a lot of interesting functionality, they bring potential problems related to privacy, information accountability and ownership of information.

Decentralized social networks have the potential to provide a better environment

within which users can have more control over their privacy, and the ownership and dissemination of their information. Therefore, online social networking will be more immune to censorship, monopoly, regulation, and other exercise of central authority. More importantly, a decentralized approach to online social networking breaks the boundaries between social networking sites by providing users more freedom to interact with each other.

6. FUTURE WORK:

- Adding the features to post, send and receive images and videos using IPFS.
- Creation of groups and assigning roles to users of that groups along with privileges.
- Provide network anonymity i.e mask user's network activity,
- Giving Cryptocurrency Incentives to Users in Exchange for Their Data.
- Introduction of Influencer Payments.
- In addition to social networks, we can support personal blogs trivially but would also like to be able to support social media like large forums(eg. Reddit), social gaming(e.g Twitch), video sharing (eg. Youtube), collaborative editing (eg.Wikipedia).

REFERENCES:

[1] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain," Business & Information Systems Engineering, vol. 59, pp. 183–187, Jun 2017.

[2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," White Paper: https://bitcoin.org/bitcoin.pdf, 2008.

[3] D. Chaum, "Blind signatures for untraceable payments," in Advances in Cryptology, (Boston, MA), pp. 199–203, Springer US, 1983.

[4] S. Haber and W. S. Stornetta, "How to time-stamp a digital document," Journal of Cryptology, vol. 3, pp. 99–111, Jan 1991.

[5] R. C. Merkle, "Protocols for public key cryptosystems," in 1980 IEEE Symposium on Security and Privacy, pp. 122–122, April 1980.

[6] D. Bayer, S. Haber, and W. S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," in Sequences II (R. Capocelli, A. De Santis, and U. Vaccaro, eds.), (New York, NY), pp. 329–334, Springer New York, 1993.

[7] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," ACM Trans. Program. Lang. Syst., vol. 4, pp. 382–401, July 1982.

[8] J. R. Douceur, "The sybil attack," in Peer-to-Peer Systems, (Berlin, Heidelberg), pp. 251–260, Springer Berlin Heidelberg, 2002.

[9] A. Back, "Hashcash - a denial of service counter-measure," 09 2002.

[10] V. Buterin, "Ethereum white paper: a next generation smart contract & decentralized application platform," https://github.com/ethereum/wiki/wiki/White-Paper, 2013.