International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

Decentralized Social Media Web3.0

Rohith Pranav Bala.C.K
First year CSE
Dr.N.G.P Institute of technology
Coimbatore,Tamilnadu
rohithpranav567@gmail.com

***Abstract*—** This paper explains resolving the issues and threats which are raised from social media by enhancing and upgrading to decentralized social network which uses hashing and smart contract that gives improved security and data privacy. The obtained decentralized network uses interplanetary file transfer protocol(IPFS) which provides robust security over data privacy. The password system used in current social media security is replaced by hashed digital signature and crypto wallets.

I. INTRODUCTION

Blockchain based social media are decentralized networking platforms built on blockchain protocols. The aim is to enable implementation of applications and smart contracts that support social networking and content creation.
A decentralized online social network (DSON) is a distributed system for social networking with no or limited dependency on any dedicated central infrastructure.

II. PROMBLEM STATEMENT

A. Social media

Social media is a technology that enables people all over the world to share their ideas, opinions, and knowledge across virtual networks and communities.

- Social networking sites
- Community blogs
- Video hosting sites
- Image sharing sites
- Social review sites
- Discussion sites

B. Threats to Privacy on Social Media

Social media users' concerns about their privacy have spiked in recent years. Incidents of data breaches have alarmed many users and forced them to rethink their relationships to social media and the security of their personal information. Criminals are adept at tricking social media users into handing over sensitive information, stealing personal data, and gaining access to accounts users consider private.

- **Data Mining**
  Everyone leaves a data trail behind on the internet. Every time someone creates a new social media account, they provide personal information that can include their name, birthdates, geographic location, and personal interests. In addition, companies collect data on user behaviors: when, where, and how users interact with their platform. All of this data is stored and leveraged by companies to better target advertising to their users. Sometimes, companies share users' data with third-party entities, often without users' knowledge or consent.

- **Phishing Attempts**
  Phishing is one of the most common ways criminals attempt to gain access to sensitive personal information. Often in the form of an email, a text message, or a phone call, a phishing attack presents itself as a message from a legitimate organization. These messages trick people into sharing sensitive data, including passwords, banking information, or credit card details. Phishing attacks often pose as social media platforms. In August 2019, a massive phishing campaign targeted Instagram users by posing as a two-factor authentication system, prompting users to log in to a false Instagram page.

- **Malware Sharing**
  Malware (malicious software) is designed to gain access to computers and the data they contain. Once malware has infiltrated a user's computer, it can be used to steal sensitive information (spyware), extort money (ransom ware), or profit from forced advertising (adware). Social media platforms are an ideal delivery system for malware distributors. Once an account has been compromised (often by obtaining passwords through a phishing attack), cybercriminals can take over that account to distribute malware to all of the user's friends or contacts.

- **Botnet Attacks**
  Social media bots are automated accounts that create posts or automatically follow new people whenever a certain term is mentioned. A large group of bots can form a network known as a botnet. Bots and botnets are prevalent on social media and are used to steal data, send spam, and launch distributed denial-of-service (DDoS) attacks that help cybercriminals gain access to people's devices and networks.

C. Social media is bad for data security

- **FAKE PROFILES AND IMPERSONATION**
  Online criminals target social platforms because your account is rife with personal information they can use for a variety of purposes [8]. The information gathered can be used against you via blackmail or to impersonate you.

- **SPAM, VIRUSES, AND MALWARE**

Social media is a better, faster way to spread malicious content like scams and malware - more so than the run-of-the-mill spam emails you see asking to help out a Nigerian prince in your inbox. If you type your login credentials into this popup, you're handing over your password and username information to the scammer. Then, the scammer uses that information to send the same video to all of your friend

III. How Blockchain Can Solve This Problems

A. How decentralized social media works

- Decentralized social networks are a class of decentralized applications (dapps) applications powered by smart contracts deployed on the block chain. The contract code serves as the backend for these apps and defines their business logic.

- Decentralized social networks exist on a peer-to-peer network comprising thousands of nodes around the globe. Even if some nodes fail, the network will run uninterrupted, making applications resistant to failures and outages.

- Many block chain-based social platforms have native tokens that power monetization in absence of advertising revenue. Users can buy these tokens to access certain features, complete in-app purchases, or tip their favorite content creators.

B. Ideas to improve social media

- **P2P communication**
  Peer-to-peer (P2P) is a decentralized communications model in which each party has the same capabilities and either party can initiate a communication session.

- **Immutable ledger**
  The word Immutable means "cannot be changed." And ledger is a fancy term for record, a record of something. Therefore an Immutable Ledger is a record that cannot be changed.

- **IPFS**
  Interplanetary File System (IPFS), social networks built on Ethereum can protect user information from exploitation and malicious use. No one will sell your personal information to advertisers, neither will hackers be able to steal your confidential details.

- **Smart Contract**

  Smart contracts are simply programs stored on a block chain that run when predetermined conditions are met. They typically are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary's involvement or time loss.

- **Digital signature**
  A digital signature is a cryptographic output used to verify the authenticity of data. A digital signature algorithm allows for two distinct operations: a signing operation, which uses a signing key to produce a signature over raw data.

- **Hashing**
  Hashing is the process of transforming any given key or a string of characters into another value. This is usually represented by a shorter, fixed-length value or key that represents and makes it easier to find or employ the original string.

C. Benefits of decentralized social media

- Decentralized social networks eliminate the "middle-man". Content creators have direct ownership over their content, and they engage directly with followers, fans, buyers, and other parties, with nothing but a smart contract in between.

- Decentralized social networks rely on decentralized storage, not centralized databases, which are considerably better for safeguarding user data.

- Decentralized social networks afford users a high level of privacy and anonymity. For instance, an individual can sign in to an Ethereum-based social network using an ENS profile or wallet—without having to share personally identifiable information (PII), such as names, email addresses, etc.

References

ethereum.org/en/social-networks/
Coinmarketcap-Decentralized social media explained