ISSN: 2347-6540
International Journal of Latest Research In Engineering and Computing (IJLREC)
Volume 9, Issue 1, Page No. 6-10, 2022
www.ijlrec.com

IMPACT OF BLOCK CHAIN FOR SOCIAL MEDIA: REVIEW

Ayushi Negi[1]
MCA Student, Uttaranchal University
ayushinegi232@gmail.com
Anuj Sundriyal[2]
MCA Student, Uttaranchal University
anujsundriyal1234@gmail.com

Abstract- ***Continues use of different social media platforms comes with the risk of privacy, which definitely lead the risk of losing the personal data or organizational data. In this research paper, we are investigating the impact (pros and con) of block chain on social media. Block chain is restoring online privacy unlike traditional database which store data at one place, Block chain creates a distributed ledger that ensure that information is safe in different hashes that connect to verify the data, Thus it assures data precision and it provide high level end-to-end encryption and security [1].So, blockchain social media provides revenue-generating opportunities to the users or content contributors also.***

Keywords: Social media, block chain, encription.

1. INTRODUCTION

WHEN BLOCK CHAIN WAS INTRODUCED

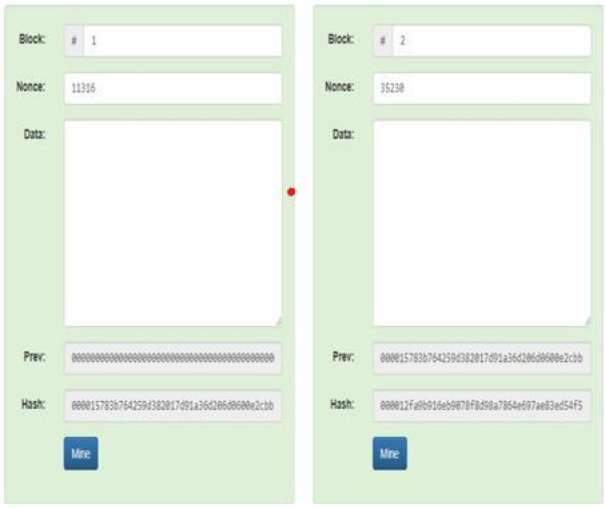
Blockchain technology was first outlined in 1991 by Stuart Haber and W.Scott Stornetta, two mathematicians who wanted to implement a system where document time stamps could not be tampered with. In the late 1990s, cypherpunk Nick Szabo proposed using a blockchain to secure a digital payments system, known as bit gold (which was never implemented). Blockchain a peer-to- peer network that sits on top of the internet—was introduced in October 2008 as part of a proposal for bitcoin, a virtual currency system that eschewed a central authority for issuing currency, transferring ownership, and confirming transactions [2].

WHAT IS BLOCKCHAIN?

Blockchain is a distributed database that is shared among the nodes of a computer network. A blockchain, like its name implies, structures its data into blocks that are strung together. This data structure inherently makes an irreversible time line of data when implemented in a decentralized nature. When a block is filled, it is set in stone and becomes a part of this time line. Each block in the chain is given an exact time stamp when it is added to the chain, as new data comes it is entered into a fresh block [3]. Once the block is filled with data, it is chained onto the previous block, which makes

HEART OF BLOCKCHAIN (SHA-256)

Sha-256 stands for Secure Hash Algorithm 256 sha-256 is used to encrypt data in the blockchain and no one can decrypt the data except the owner of the data and Sha-256 was developed in2001 by National Security Agency.
SHA-256 is a patented cryptographic hash function that outputs a value that is 256 bits long. Hashing is a technique that is used for encryption of data which we want to make secure Basically in hashing technique data is encrypted and make that encrypted data address of the block and it is not possible to decrypt the encrypted data. The data chained together in chronological order. One key difference between a typical database and a blockchain is how the data is structured. A blockchain collects information together in groups, known as blocks, which hold sets of information.



WHY BLOCKCHAIN IS USED?

Blockchain provide improved accuracy by removing human involvement in verification, the cost is also reduces by eliminating third-party verification, it also provide secure, private, and efficient transactions, it also provide transparent technology [4].

HOW BLOCK CHAIN LOOK LIKE

Block chain is simply a very long string of 1's and 0's. Every 10 minutes a new block gets added to the chain, that's the reason behind the name Blockchain [5].

WHAT IS SOCIAL MEDIA?

Social media is a computer-based technology that facilitates the sharing of ideas, thoughts, and information through the building of virtual networks and communities. Social media originated as a way to interact with friends and family but was later adopted by businesses that wanted to take advantage of a popular new communication method to reach out to customers. The power of social media is the ability to connect and share information with anyone on earth, or with many people simultaneously, some example are YouTube, Facebook, WhatsApp, and Instagram. Social media originated as a way to interact with friends and family but was later adopted by businesses that wanted to take advantage of a popular new communication method to reach out to customers. The power of social media is the ability to connect and share information with anyone on Earth, or with many people simultaneously [6].

CYBER CRIMES THAT OCCUR IN SOCIAL MEDIA

Social media is a weapon that is capable of construction as well as destruction. The real power of the prevailing social media platforms becomes evident by witnessing the influence created by these platforms on a large scale [7]. Technology while

providing so many advantages poses threats to individuals and social media has become a haven for the criminals as it has given rise to crimes committed in the online world [8]. With this changing nature of communication, criminals are using social media websites for their own malevolent motives. The report of NW3C discussed six crime types using social media [9]:

1) Burglary via social networking: Here criminals search social media for a potential target for burglary. Social media users usually post their personal activities, for example, they are having dinner or going somewhere for vacations. Criminals look for this type of information to find easy targets, where they find large time frame to burgle the property [9].

2) Social engineering and phishing: Social engineering uses psychological manipulation to get personal information [9]. People using social networking sites receive messages from their friends requesting immediate financial assistance. Actually, these messages were not sent by their friends, but by the criminal who stole their friends' emails and passwords [10].

3) Malware: Social media provides a great platform for spreading viruses and malware. Developers of adware, malware and viruses hide their destructive programs in links, attachments and messages, which are a normal task in any social networking website. Once users respond to them, the malware infects their computer without their knowledge [10].
Cyber-stalking: The stalking inside the cyber world by using the social media or any other online medium, which may cause feelings of irritation, abuse and emotionally anxiety to the victim, is cyber-stalking [11].
6) Cyber-casing: The Report on Criminal use of Social Media by the National White Collar Crime Centre [9] explains cyber- casing as a process, which is used to produce real world location using various data available in online resources. One of the prominent features that social media sites have offered in recent years is geo-tagging [9]. With widespread use of mobile applications, geo-tagging is a major trend of social media sites [12]. Mobile applications have played a vital role in promotion of this trend without any legal purpose [12]. Geographical information is the prime element in the process of cyber-casing, which helps criminals plan and execute their mischievous plans [12].

HOW BLOCK CHAIN HELP SOCIAL MEDIA

1 Data Storage

The times when knowledge was available only to the chosen ones are long gone. In the digital age, it is much harder to cut yourself off the non-stop information stream than getting the information you need. With the emergence of Facebook , the development of artificial intelligence and machine learning, the amount of information that needs to be stored is continuously growing.

Big Data challenges the capacities of modern data centers significantly. As the technologies mentioned above develop further, the data storage situation gets tougher. IDC predicts that the world will have 163 zetta_bytes of data to store by 2025. Current cloud storage services do not have the potential to deal with such vast amounts of information effectively.
Blockchain can potentially solve the data storage issue thanks to its decentralized and distributed nature. To store the data in the blockchain, one will need to break it in small parts. Every part will be encrypted and uploaded to the blockchain. Next, the data will be distributed in a way that will allow accessing all of it even in case a part of a network does not function. Such data handling can serve as a much better alternative to cloud storage**.[13]**

2 Data Security

Storing data in blockchain will bring vast improvement to data security. Currently, the cloud data is stored in centralized storage units, which makes it sensitive to any security breach. Blockchain can enhance the safety and speed of cloud storage. The data, stored in the blockchain, will be stored across the nod network. There will be no need to rely on a central entity or location in this case. Any data attack will not be potentially fatal in the blockchain storage. There will be no way to tamper or steal the data, stored in the blockchain. Storing data in the blockchain will secure it from force-major circumstances that damage and destroy centralized databases at present (e.g., natural disasters, riots, political escalation). A distributed blockchain data storage network will store redundant copies of data among different nodes so that there is no data downtime and loss no matter what. Blockchain has the potential to store, process, and manage data without the need to rely on any third party.**[13]**

3 Transaction on Social Media

On the blockchain, the process of transaction verification and recording is immediate and permanent. The ledger is distributed across several nodes, meaning the data is replicated and stored instantaneously on each node across the system. When a transaction is recorded in the blockchain, details of the transaction such as price, asset, and ownership, are recorded, verified

and settled within seconds across all nodes. A verified change registered on any one ledger is also simultaneously registered on all other copies of the ledger. Since each transaction is transparently and permanently recorded across all ledgers, open for anyone to see, there is no need for third-party verification**[14]**

4 Block Chain in Cyber crime

The year 2017 saw the proliferation of cyber crimes[15], with ransomware being the most notorious of such crimes. The likes of "WannaCry" and "Bad Rabbit" took over numerous computers all over the world, threatening its users with harm, usually by denial of access to data. The attacker demands a ransom from the victim, promising
– truthfully or not – to restore access to the data upon payment of "ransom". The modes of cyber attacks are varied: hackers may use email attachments to embed malware, they may pose as customer support to obtain user log details or they may resort to phishing to obtain an unsuspecting user's sensitive personal information. Stealing sensitive information is not the only modus operandi of cybercriminals; they can also undermine business through information sabotage and the spread of fake data to cause system failures. Whatever the method used, the basis of their strategy is consistent: exploiting weak points in security systems[16]Traditionally, organizations store information in highly centralized systems. Unfortunately, recent cybercrime cases have shown the inherent vulnerability of centralization, especially when it concerns personal data security. The Equifax data breach in the summer of 2017, where the personal information of approximately 143 Million Americans may have been stolen, is such an example.[17]
This is where blockchain technology or distributed ledger technology comes in. The emergence of blockchain as a development platform has given rise to decentralized services. As opposed to a centralized approach, these new services rely on the blockchain's distributed network that may be used for a variety of purposes, including cybersecurity.[18]
Blockchain opens up new ways to combat the rampant threat of cybercrime in a variety of ways, one of which is data storage protection. By storing and sharing information via the distributed ledger or record technology, institutions and businesses can ensure that there is no single way which hackers could steal data. Information, through distributed records, can be decentralized, and sequentially hashed and encrypted – making it almost impossible for intruders to make sense of information.[19] Think of it as a one thousand piece puzzle. By hacking a centralized system, an intruder can access all one thousand pieces in one go. In real life this could mean getting the personal details of around one thousand individuals just through one security breach. With a decentralized system, cyber criminals can only access one piece at a time, making it much more time consuming and nearly impossible to see the whole picture. They would have to hack a variety of gateways multiple times in order to acquire someone's personal information. This would give the security system enough time to identify the source of the vulnerability and contain the breach.[20]
This principle may also be applied to create distributed network security to safeguard vital external infrastructure, such as domain name services (DNS) for company websites. The attack that took down Twitter and Spotify in 2016 illustrated the vulnerability of the current DNS practice of keeping the access key on only one server and relying on caching[21]. A blockchain-based server would minimise the risk by creating a wider network of security keys. Imagine a chest with multiple locks. Before it can be opened, all the locks should be unlocked using different keys that could be hidden anywhere. This is the underlying logic behind the decentralized approach to network security.[22] Of course, in addition to protecting the data itself, the method of information sharing should also be shielded from cyber attacks. For example, instant messaging tools such as Facebook Messenger or WhatsApp ,through , already armed with in-app security measures, still have weak points in terms of security. WhatsApp, though it has end-to-end encryption to protect the contents of messages, still collects metadata (information about who the user is talking to). Such metadata is frequently stored in single systems, presenting a vulnerability that hackers will surely take advantage of. To solve this problem, blockchain technology can decentralize the network itself and divide the metadata – thereby making sure that they cannot be assembled in one place.
From a cybersecurity point of view, blockchain technology offers a new way to think about system design that disincentivizes cyber-attack. It is akin to the difference between a community storing all their money in a central bank and each person keeping their own money at home. While a bank has security systems it is also an obvious target for bank-robbers who want to make a big windfall.

REFERENCES

[1] https://www.benzinga.com/node/24179905
[2] https://en.wikipedia.org/wiki/Blockchain
[3] https://www.investopedia.com/terms/b/blockchain.asp#toc-what-is-a-blockchain
[4] https://www.investopedia.com/terms/b/blockchain.asp#toc-pros-and-cons-of-blockchain
[5] https://www.linkedin.com/pulse/how-does-block-blockchain-look-like-vijay-raghunathan

[6] https://www.investopedia.com/terms/s/social-media.asp
[7] Analysis of Cybercrime on Social Media Platforms and Its Challenges
[8] Afrah Almansoori1,3 , Mohammed Alshamsi2,3, Sherief Abdallah3, and Said A. Salloum4, Influence of Social Media and Growth of Cyber Crimes – A Study MS. NEHA GUPTA1
[9] NW3C, "Criminal Use of Social Media (2013)," NW3C, 2013.
[10] Social Media-Related Cybercrimes and Techniques for Their Prevention Tariq Rahim Soomro1* , Mumtaz Hussain
[11] College of Computer Science & Information Systems, Institute of Business Management, Karachi, Pakistan 2 Freelance programmer, Karachi, Pakistan NW3C, "Cyberstalking (March 2015)," NW3C, 2015
[12] P. Saariluoma and H. Sacha , "How cyber breeds crime and criminals," The Society of Digital Information and Wireless Communications (SDIWC), 2014.
[13] https://www.goodfirms.co/blog/problems-blockchain-solves
[14] https://towardsdatascience.com/blockchains-the-technology-of-transactions-9d40e8e41216#:~:text=When%20a%20transaction%20is%20recorded,other%20copies%20of%20t he%20ledger.
[15] Richard van Hooijdonk, "Cybercrime may be the biggest global threat of 2018", https://www.richardvanhooijdonk.com/en/blog/cybercrime-may-be-the-biggest-global- threat-of-2018/, Accessed 06 August, 2018
[16] Catherine Luff, "Cybersecurity and the future of blockchain technology", http://www.gingermaypr.com/cybersecurity-blockchain-technology.htm, Accessed 10 August 2018.
[17] Paul Worrall, "Blockchain: the solution to the cybercrime epidemic?" https://www.ibtimes.co.uk/blockchain-solution-cybercrime-epidemic-1660702, Accessed 09 August 2018.
[18] Ralph Tkatchuk, "Is Blockchain the ultimate weapon against cybercrime?" http://dataconomy.com/2017/10/blockchain-ultimate-weapon-cybercrime-2/, Accessed 07 August 2018.
[19] Catherine Luff, "Cybersecurity and the future of blockchain technology", http://www.gingermaypr.com/cybersecurity-blockchain-technology.htm, Accessed 10 August 2018.
[20] Paul Worrall, "Blockchain: the solution to the cybercrime epidemic?" https://www.ibtimes.co.uk/blockchain-solution-cybercrime-epidemic-1660702, Accessed 09 August 2018.
[21] An area or type of computer memory in which information that is often in use can be stored temporarily and reloaded very quickly
[22] Catherine Luff, "Cybersecurity and the future of blockchain technology", http://www.gingermaypr.com/cybersecurity-blockchain-technology.htm, Accessed 10 August 2018.