BLOCKCHAIN AND PRIVACY PROTECTION - CONCERNS AND CHALLENGES

Yogini Upadhyay
Ph.D. Scholar
Jagran School of Law
Jagran lakecity University, Bhopal (M.P.)

ABSTRACT

Objectives of the present research paper is to highlight the blockchain technologies, as an example of extreme decentralization. By analyzing the different aspect of decentsolized approach we see that there is a widespread adoption of blockchain technology for its ability to increase user privacy, data protection and data ownership. But at the same time, the more we shift towards a decentralized infrastructure, the less we used to rely on trust and the more we rely on transparency. If decentralization can contribute to promoting users privacy and autonomy, it might, however, come to at the cost of radical transparency. Therefore, it is clear that there is need to enhance the blockchain technology so that balance can be made between trust and transparency in privacy communication.

Key Words: *Blockchain Security,Decentralized infrastructure,*

INTRODUCTION

With the recent state of telecommunication technologies, it is really difficult to communicate on the Internet without disclosing information to centralized third parties, be they either governments agencies or private corporations. The privacy of communication go into peril in a variety of ways, depending on the types of approaches at hand. In most centralized system, users do not need to worry about securing their own communication channels, which are usually controlled and managed by a trusted central authority. This central authority has complete access to everyone's communications, surveillance remains, almost inevitably most important threat to privacy. Majority of the internet traffic is routed through a few centralized series, controlled and governed by a few large companies. Moreover, most centralized platforms rely on unifying network points that can be regarded as single points of failure, to the extent that they are more likely to be attacked by malicious users, or simply be coerced by governmental agencies in order to disclose information about specific users[1].

There is a growing interest in decentralized architecture as a way to protect one's privacy against the growing authority and surveillance of centralized third parties. Decentralized architectures are much more supportive of individual freedoms, such as privacy and freedom of expression[2]. Block chain technologies is an example of extreme decentralization. Blockchain is gaining impectus because it guaranties more reliable and expedient services. Therefore it is important to consider the security and privacy issues and challenges behind the innovative technology.

Privacy is a qualified right, essential to autonomy and the protection of human dignity, serving as the foundation upon which many other human rights are built[3]. Before discussing about blockchain it would be pertinent to distinguish two possible approaches, centralized and decentralized.

CENTRALIZED ONLINE APPROACH

Internet grew into more and more centralized clusters governed by a few large corporations. eg Google or Facebook. These services use decentralized infrastructures, yet, their governance model is highly centralized. Inspite of the

benefit it provider in terms of coordination and control, the concentration of power in the hands of a few online service providers in increasingly leading to a situation of very common surveillance[4].

In centralized systems coordination can easily achieved, where information is routed through a series of trusted nodes that collect information needed to coordinate network's activities. Information is processed centrally and then send to each individual user on a selective basis to ensure the proper operations of the network. Centralized coordination thus provide two important benefits: first, it reduces the number of transactions necessary to coordinate a group of individuals, secondly it reduces the amount of unnecessary disclosure that users would otherwise have to tackle with in a more decentralized system.

The drawback is, of course, that centralized coordination comes at the cost of entrusting a centralized third party with managing all users activities and communication[5]. Yet, sometimes, these centralized authorities are not worthy of trust. The reason is that centralized coordination could potentially lead to some abuses of power by large online operators, to the extent that they control the operations of the network, online operators are often tempted to impose certain number of obligations on all users participating to a network, which are forced to accept these conditions in order to benefit from the service, even if this goes against their own interest. Centralization also provide more room for top down regulation and control. They have full control over the operation of the platform; perhaps even more critical is the fact that online operators rely on technological means in order not only to monitor, but also dictate how people can or cannot interact with their platform thereby reducing the autonomy and infringing upon the privacy of users.

Today our interactions are for the most part mediated by a variety of connected devices that communicate information to one or more internet service providers, to the extent that they collect relevant data concerning users activities and online communication. In this way contralised online plateforms constitute very valuable sources of information, which can be exploited by both ill intentioned hackers and governmental agencies. Besides, most centralized operators are subject to the regime of intermediaries liability limitations, designed to promote

cooperation between the government and online operators encouraging them to disclose the information about alleged infringers in order to escape from potential liability claims.6

DECENTRALIZED ONLINE APPROACH AND BLOCKCHAIN

As a reaction to the growing centralization of data in the hands of few large online service providers, decentralized and federated system have emerged in recent years. Decentralized networks include the peer to peer file sharing networks Bit Torrent, the decentralized communication system, Fire chat and the decentralized payment system Bitcoin, based on blockchain technologies. These platforms are also more likely to protect the privacy and confidentiality of information since there is not centralized intermediary that controls all the information flows. Yet, given that no central entity is in charge of coordinating users behavior, information needs to be disclosed to a distributed network of peers to effectively align action in the network Calloway, 2004. Decentralized networks thus require more transparency in order to effectively coordinate activities between the network nodes.

BLOCKCHAIN

Blockchain technology secures and authenticate transaction and data through cryptography. Therefore, we first recall what cryptography is and then introduce the concept of blockchain as a protocol for transmitting information in a secured way.

Cryptography is a discipline dedicated to protecting messages by ensuring confidentiality authenticity and integrity using keys. There are several types of cryptography's algorithms : the classical cryptography which is easily decipherable, systemic cryptography algorithms with a secret key and asymmetric cryptography algorithms with public or private keys. In the latter case, the public key allow the encryption and the private key the decryption. There are several asymmetric cryptographic algorithms including RSA (encryption and signature), or DSA (signature). Asymmetric cryptography is used to ensure the authenticity of a message. The signature of the message is encrypted using private key attached to the message. The recipients then decrypt and cryptogram using the

public key and normally retrieve the signature. This ensures that the sender is the author of the message. When a message is encrypted. it is then transferred through secured protocols. With the internet (TCP-IP) there are already computer protocols that allow the creation of an infrastructure that transfers data packets from one point to another point[6]. Now we come to blockchain.

Blockchain technology appeared with a white paper written by an anonymous person or group called Satoshi Nakamoto, but after that it has been catching on line wildfire. Blockchain is a secure, transparent technology for storage the transmission which operators without a central control device that can be used to transfer data from point A to point B. It is a distributed and public shared database that manages a list of records mechanically protected against tempering or modification by storage in nodes through its decentralized timeline. It is a database, contains the history of all the exchanges between the users since its creation. It is shared by its various users, without intermediaries, which allows each one to check the validity of the channel. This method uses energy or a means of verification that the miner has done a good job.

Indeed, blockchain represents an important and promising development in internet technologies insofar as it makes it possible for people to transact and to interact with one another without relying on any centralized intermediary. Moreover the blockchain is an immutable, anonymous, unshakable and decentralized ledger. It is a public share database that records transactions between two parties. Blockchain document and confirm owners at a particular time through cryptography. After a transaction is validated and cryptographically verified by other participants or nodes in the network, it is made into a block on the blockchain. A block contains information about the time the transaction occurred, previous transaction, and detail about the transaction. Once recorded as a block, transaction are ordered chronologically and cannot be altered. After the creation of Bitcoin, this technology rose to popularity. Bitcoin is the first example where the blockchain technology has been used and later in other cryptocurrencis.

There are two types of blockchain one is public and the other is private. A blockchain is called public if each participants can read it and use it to carry out transactions but also if everyone can participate in the process of creating the

consensus. There is therefore no central register, not a trusted third party. On the other hand, a blockchain is called private if the consensus process can only be achieved by a limited and predefined number of participants. In this case, the consensus process is controlled by a preselected set of nodes. The private blockchain does not used necessarily mechanisms based on cryptsgraphy. Private blockchain are different from public blockchains, which are available to any node that wishes to download the network. A hybrid blockchain contains characteristics of private and public blockchain[7].

IMPACT OF BLOCKCHAIN ON PRIVACY AND AUTONOMY

With the rise and widespread adoption of technology, data breaches have become frequent. User information and data are often stored, mishandled, and misused, causing a threat to personal privacy.

Granting that the features of blockchain technology guarantee more reliable and expedient services, it is important to consider the privacy issues and challenges behind the innovative technology.

Due to its nature decentralization, transactions and data are not verified and owned by one single entity as they are in typical system, rather, the validity of transactions are confirmed by any node or computer that has access to the network. The decentralized architectures are actually intended to preserve and to promote users privacy by focusing on at least one of two different privacy concern; confidentiality and control. The former is meant to ensure the confidentiality of people's personal data by ensuring that their interactions and online communications are shielded from the eyes of third party. People are thus granted a means to escape from the surveillance of the government agencies and from the prequent data collection of existing commercial offerings. For instance TOR and Fire chat it designed to enable people to more actively decide when and with whom to share their own personal information. Rather than four sing on the concealment of personal data, it empowers individuals with a greater degree of control over the collection and use of their data in the context of their ongoing interactions with third party online operators. Initiative of this kind

include, for instance, the various personal data store initiatives, such as personal Black box and IDZ,s open mustard seed[8].

Blockchain has been acknowledged as a way to solve fair information fractions, a set of principles relating to privacy, a set of principles relating to privacy practices and concern for users. Blockchain transactions allow users to control their data through private and public keys, allowing them to own it. Third party intermediaries are not allowed to misuse and obtain data. If personal data are stored on the blockchain, owner of such data can control when and how a third can access it. In blockchain, ledgers automatically include an audit trail that ensures transactions are control when and how a third party can access it.

When it comes to autonomy, decentralized architectures also have an important role to play by climinating users dependany towards centralized online operators. This is well illustrated by the Freedom Box initiative a personal serves aiming to preserve privacy an individual autonomy by providing a secure platform for personal data storage and applications deployment.

CHALLENGES AND CONCERNS REGARDING BLOCKCHAIN PRIVACY.

Due to blockchain's decentralized nature a central authority is not checking for malicious users and attacks. Although many advocates for the adoption of blockchain technology because it allows users to control their own data and exclude third parties. Moreover certain characteristics of this technology infringe on user's privacy.

Because blockchain are decentralized and allow any node to access transactions, events and actions of users are transparent. Users might be able to hack the system anonymously and escape. Because public blockchains are not controlled by a third party, a false transaction enacted by a hackers who has a users privacy key cannot be stopped. However blockchain ledgers are shared and immutable it is impossible to reverse a malicious transaction.

Most importantly, given that ill intentioned users might be tempted to cheat the system, in absence of a central authority incharge of policing the network, there needs to be a mechanism for the network to collectively verity the legitimacy of every individual transaction which require a high level of transparency in the

network. In this was the case a users transaction history would be accessible to anyone, resulting in what we consider to be a lack of privacy.

Blockchain transactions allow users to control their data through private and public keys storing the private key on a computer, flash drive or telephone can pose potential security risks if the device is stolen or hacked. If such a device lost, the user no longer have access to the crypto currency. Storing it on physical media, such as a piece of paper, also leaves the private key vulnerable to lose, theft or damage[9].

CONCLUSION

As technology develops, new opportunities are offered to use in terms of communication and information sharing. The privacy of communication can be jeopardized in a variety of ways depending on the types of approaches ie centralized and decentralized. Blockchain is a decentralized system that are actually intended to preserve and to promote users privacy. Although its scalability, security and sustainability can be questioned. The spectrum of blockchain ranges from financial, healthcare, automobile, risk management, internet of things to public and social services. In this way blockchain is data structure is utilized in various applications. Once recorded as a block, transactions are ordered chronologically and cannot be altered, therefore, this suggest that this technology is not compatible with GDPR (General Data Protection Regulation) in the European Union. There is need to found technical solution what may enable the deletion of personal data, while maintain the integrally of a blockchain.

REFERENCES

1 http://www.schneier.com

2 Zicardi G (2012) Resistance, liberation technology of and human rights in thedigital age (Vol. 7) spnires science Business Media.

3 *www.gilc.org/Privacy/Survey/intro.htm*l.

4 *https://arxiv.org/abs/180206993 A Survey on the Security of Blockchain Systems.*

5 Duftany. J.L. (2012) Cloud computing security and privacy. In 10th Latin andCaribbean conference for Engineering and Technology PP-1-9.

6 https://www.thetaxadviser.com/issues/2018/oct/crvntocurrency-comoliance challenges-irs-enforcement.html

7 https://halshs.archives-ouvertes.fr/halshs-01524440 Public Blockchain versus Private blockchain.

8 The interplay between decentralization and privacy : the case of blockchain technologies - Primavera De Filippi.

9 https://en.wikipedia.org/wiki/Privacy and blockchain.

******