BLOCKCHAIN AND DIGITAL IDENTITY VERIFICATION: NAVIGATING LEGAL IMPLICATIONS AND REGULATORY CHALLENGES

Prakrutirupa Panda*

INTRODUCTION

In this digital era, identification authentication has turned out to be an essential aspect for all online systems such as banking and shopping on the internet. But then again, there are many problems with conventional techniques of identifying people including databases that are always accessible but vulnerable to cyber-attacks, personal space threats, and slow operations. As a solution to these issues related to the verification process through which we can prove our identity digitally, blockchain presents itself as a changing method of managing our own identities on the net because it's decentralized in nature, has nothing hidden from anyone, and cannot be changed once recorded. In 2008, Satoshi Nakamoto first introduced it as a technology behind Bitcoin; since then, blockchain has grown much larger than money only used in online exchanges, basically, it can change how people prove who they are with more security than ever before. Today, it holds the potential to transform identity verification, providing enhanced security, privacy, and efficiency.

In essence, blockchain uses a decentralized network of computers to securely and transparently manage all records. It helps to solve many problems associated with conventional modes of confirming identity such as increased plight of personal data theft and enhanced user agency on such data. To be able to use this technology in an organization or for a person, it is important to look at what the law has to say about blockchain with respect to the privacy and security aspects of digital identities since there have been more individuals and organizations appreciating its benefits ever since.[1]

This piece of writing investigates how digital identification checks may be revolutionized by blockchain development. In particular, this article addresses some main aspects of blockchain technology, its types, and the increased demand for more effective methods of handling identities. Legal challenges and implications faced when adopting such identity

*BBA LLB, SECOND YEAR, CHRIST UNIVERSITY, BENGALURU.

[1] Definition and Importance (Anon. Digital Identity: an emergent legal concept. *Open Access*. https://library.oapen.org/handle/20.500.12657/33171 4 August 2024

systems based on blockchain are discussed here as well. Besides that, a discussion on how such a kind of tech can promote people's security, confidentiality, and faith in cyberspace has been provided.

Keywords: Blockchain, Digital Identity Verification, Legal Compliance, Regulatory Framework, Data Protection.

UNDERSTANDING DIGITAL IDENTITY

Digital identity means a group of digital information that is unique to each person in the space of the internet. This information could also be made up of things such as user IDs, secret codes, online profiles, purchase history, and patterns based on one's individual biological characteristics such as fingerprinting or voice. The importance of digital identity has made it an inseparable part of several transactions through which people verify who they are.

Without this form of identification, accessing financial services such as bank accounts online; making use of government portals; and using different accounts on social media websites has been difficult. Digital identity means a group of digital information that is unique to each person in the space of the internet. This information could also be made of by things such as user IDs, secret codes, online profiles, purchase history, and patterns based on one's individual biological characteristics such as fingerprinting or voice. The importance of digital identity has made it an inseparable part of several transactions through which people verify who they are. Without this form of identification, accessing financial services such as bank accounts online; making use of government portals; and using different accounts on social media websites has been difficult.

CURRENT SYSTEMS: LIMITATIONS AND VULNERABILITIES

To this day, however, the current systems for managing digital identities have many limitations and are also vulnerable. For example, they are often based on identity-controlled centralized databases, so it is much easier to launch cyber-attacks and get data from them. In turn, when hackers manage to break into such centralized repositories, they may cause damage to the private lives of millions of users resulting in identity theft and money fraud.

There are also worries regarding user control and privacy when it comes to centralization. When describing this phenomenon, emphasis should be given to the fact that many people

have no power over what happens with their personal information such as storing, collecting, or sharing it. Therefore they find themselves compelled to put faith in organizations that hold their data hence creating room for various kinds of data concerns including the misuse of information or unauthorized entry into it. Furthermore, those using different sites have multiple usernames and passwords hence end up suffering from password fatigue which exposes them to phishing scams as well as other forms of theft through hacking.

According to Dr Clare Sullivan, identity is in a new legal way in her study about digital identity handled from legal perspectives. A clearer picture of this entity can be observed with national identity schemes and examples can be found in the ited Kingdom and India. In cases where there is no formal national identity scheme lin like Australia, it could still be observed there is some legal concept of identity that is in a way coming to light. On the same note, there exist also proprietary schemes run by banks and other businesses.[2]

The digital identity of an individual, particularly one that has anything to do with commercial interaction, plays critical roles that grant it legal personality. Sullivan (2013) argues that digital identity has features of property and should be accorded legal protection accordingly. It is here that identity theft could be understood as a crime against this digital property. The study focuses on the evolution of rights and obligations concerning digital identity; including a new right for digital identity and its legal protection. Dr Sullivan states that every person should have an accurate and functioning digital identity along with the right to privacy which comes first on its own. Therefore, since it is public in nature, identity offers more privileges than privacy does hence better protection than privacy itself. The conclusion is that this approach moves from privacy to identity in legal theory and subsequent practices.

Real-life cases examined in the research show what this means for people, companies, and policymakers. A significant shift in the way digital identity is viewed in law and users' perceptions about it is suggested by the results, pointing out that it is like an asset that cannot be taken away from anyone or misused easily.[3]

Current systems of digital identity are vital to contemporary online engagement but do have pitfalls including centralization, vulnerability to breaches, and well no user control over

[2] *Digital Identity: An emergent legal concept*. Available at: https://library.oapen.org/handle/20.500.12657/33171 (Accessed: 04 August 2024).
[3] *Digital Identity: An emergent legal concept*. Available at: https://library.oapen.org/handle/20.500.12657/33171 (Accessed: 04 August 2024).

them. Analyzing these facts makes clear why it should be acknowledged as both a legal entity and relevant property; this would require stronger legislative measures against these problems so as to guarantee secure and trustworthy identification verification processes online.

HOW BLOCKCHAIN ADDRESSES IDENTITY VERIFICATION

Since its inception in 2009, blockchain technology has fundamentally changed how we conduct our lives online and one of its most promising applications is in identity verification. Identity verification, which is perhaps one of the leading applications for blockchain technology,[4] is tackling longstanding problems that have plagued traditional identity verification methods through the use of decentralization principles, transparency, and improved safety measures.

Decentralized Identity

One of the primary benefits of blockchain is that it gives users full control over their identity data, thereby cutting down dependence on centralized authorities and minimizing the chances of getting hacked. It makes it possible for reformers to manage and share their identity information directly, thus enhancing privacy and security. In this way, every person decides on her own when to allow use of data and to whom, so as to help people protect personal information better than they have ever done before.

Transparency and Trust

To guarantee openness and verification, all sorts of transactions and data stored on public blockchains can be checked by everyone inside the system, thereby creating a trusting environment. Public records are totally transparent whereas those that are private tend to have partial visibility enabling a balance between secrecy on one hand with protection from outside threats for businesses. With such selective transparency, authorized users can see as well as validate but cannot disclose classified data.

Enhanced Security

These days, we are living in a world where the rapid development of technology has made

[4] Careja, A.-C. & Tapus, N. (2023). Digital Identity Using Blockchain Technology. *Procedia computer science*. 221. p.pp. 1074–1082. Available from: [Accessed: 5 August 2024].

us realize that there is no limit to what can be achieved. One area is decentralization which is what blockchain is based upon. Blockchain does not have a main server or point where all information goes through; hence it lacks a single point of failure. This greatly reduces the chances of any hacker getting in. The operation of this system relies heavily on a proof-of-work algorithm that requires huge amounts of computational resources to solve mathematical puzzles (porous locks). Data integrity is ensured by these cryptographic hashes while their unauthorized modification becomes almost impossible as well as too tedious even for an individual person.[5] They claim that altering one blog block one fly would mean redoing all other blocks situated after it and if you were a mathematician from another planet, you still wouldn't be able to do that alone. Moarecoverra, a decentralized ledger requires every member to keep a copy of today's version thus making it very unlikely for someone who wants to change something in to chain to access everyone's computer.

User Control and Reduced Costs

Blockchain technology empowers users to independently manage their information, therefore reducing expenses related to identity verification through traditional means. Traditional cryptographic systems have a single point of truth h in the form of a certificate authority and if this entity gets compromised it can cause a catastrophe. In contrast, the blockchain method denies such a vulnerability by sharing the responsibility for maintaining its books amongst all participants. By virtue of this process, modifying one reference system would be extremely difficult; hence maximum protection is achieved.

APPLYING BLOCKCHAIN TO AUTHENTICATION AND LEGAL IDENTIFICATION

Fabulous firms are applying the possibilities of blockchain to come up with a plethora of services regarding Blockchain IDs. Essentially, each blockchain ID is a certain information piece on the chain that can be verified by any third party and shows details like date of birth. This verification depends on the Elliptic Curve Digital Signature Algorithm (ECDSA). When one adds his/her ID to the blockchain, an identity issuing service associates its public key to the ID by default and transfers out all rights related to its private key to the user. Then, people can use it for signing in such a way that their signatures can be checked against keys

[5] Careja, A.-C. & Tapus, N. (2023). Digital Identity Using Blockchain Technology. *Procedia computer science*. 221. p.pp. 1074–1082. Available from: [Accessed: 5 August 2024].

placed in the blockchain. As such, this mode of sign-in has no other owner besides itself that serves as an independent source of proof without belonging to any single person or organization.

Innovative organizations are taking advantage of what cryptocurrency technology has been able to offer as they create multiple products revolving around blockchain ID. Essentially, as a blockchain ID it can get noticed from the chain, the verification of which any third party can do shows needful details like date of birth. Such verification employs The Elliptic Curve Digital Signature Algorithm (ECDSA) whose concept is to undertake in issuance of identity. When an individual adds their ID number to the blockchain, a service is default binding its public key with this account and transferring ownership to the client who has its private one. This allows users to sign texts with a signature that can be validated based on what's stored on the blockchain only by means of someone else's public keys which are common among all who participate in this network but nobody has them specifically attached or related only to him or her. Thus, this kind of authentication system acts as a single sign-on portal that may be accessed through any application.

The implementation of blockchain in identity verification comes with several challenges. Therefore, technical, regulatory, and user adoption barriers should be surmounted for blockchain-based identity verification systems to fulfill their potential. However, there are many reasons for considering blockchain as a better option for future digital identities; its perquisites include reduced fraud rate, enhanced privacy, y, and efficient identity control. It is apparent that as we move further into the digital age there will be a need for a major reform of our existing identification systems and this calls for exploring the possible solution through blockchain.

Legal Implications of Blockchain-Based Digital Identity

The involvement of blockchain technology in digital identity management presents a complicated mix of legal factors, more so when it comes to traditional ideas of identity and personhood. Conventional legal structures at international and national scales have not yet completely embraced or dealt with the ramifications of blockchain's decentralized form vis-a-vis identity management.

The Concept of Identity in Law

From the legal standpoint, it consists of different facets including group,s and is frequently associated with the larger understanding of being a human being. Examples of these include but are not limited to, one's right to have contracts or enjoy parental recognition or even their voting rights as well as holding a public office. This legal personhood which is of great importance describes laws dealing with such subjects as a "device for technicalities" rather than being at the heart of any legal transaction. The conventional view on identity which can be seen in identity cards and passports has always been envisaged together with citizenship – an idea that although appears simple at first sight; requires a deeper probe into various intricacies involved in its application.

International and National Legal Contexts

International law and national law intersect closely, especially in human rights. With regard to ensuring that nobody ends up stateless, a state has a very important responsibility for citizenship and identity papers. The right to be recognized as a person before the law has been guaranteed by Article 16 of the International Covenant on Civil and Political Rights (ICCPR). This recognition serves as a prerequisite for accessing different entitlements and obligations such as the right to life itself; personal inviolability or bodily integrity; privacy; freedom of conscience or thought; and political participation.

According to law enforcement bodies principles that define the structures to ensure compliance with property rights standards, with regards to social norms on identity ownership relate also to local ownership massacres. Indeed one would argue that there exist different forms of identity ranging from those locales and ethnics where they have no state representation what so ever as happens in African countries including Angola, Guinea-Bissa, or Mauritania; which have always been subjectively constituted as objects of global systems by Europeans and Americans alike; yet for some people there is still coexisting with their own countries without much sign of contagion from such virtual ellipses within which impulses continue despite everything else fading away into oblivion other than fading away into oblivion without leaving any traces behind them whatsoever since then capitalism emerged functioning almost as the 'face' notwithstanding selling highly coveted 'black' commodities from developing nations very cheap despite the appearance on your computer screen that everything has returned back new again after logging off at different times than

ours.

Blockchain's Impact On Legal Identity

Blockchain technology offers a novel approach to managing digital identities, providing enhanced security, transparency, and user control. However, its implementation raises several legal questions:

- Legal determinacy of identity: The decentralized nature of blockchain often raises challenges against conventional legal systems which have relied on central bodies for determining identities. Consequently, there is a need for re-examinations on approaches toward establishing and acknowledging legal personhood in a decentralized environment.

- Rights and Ownership: When it comes to blockchain technology, the issue of data ownership is brought to the forefront more than ever before. In addition, although it is safe to use blockchain for managing personal information, its legal implications regarding ownership and access remain unclear. The decentralized nature of identity records maintained in blockchains questions the limits of individual data rights as opposed to those of relational data.

- The socio-legal thresholds of identity might be redefined by blockchain technology as it harmonizes an individual's data ownership with the relational dimensions between various players. This is an important consideration for ensuring that identity systems based on blockchain conform to current legal doctrines and respect for human rights

- Integration of Philosophy and Law: The spirited argument about identity is complex whether it is considered as a personal or a relational construct; and therefore, it mixes up with legal demands. In order to satisfy individual rights as well as the larger socio-legal dimensions, blockchain must handle these intricate entanglements.

LEGISLATION OF DIGITAL IDENTITY INFORMATION

In this article, our aim is to outline and articulate the changing dynamics in the management of digital identity. After showcasing some of the most promising use cases in both public and private sectors, we turn to discuss the possible consequences of these innovations on the

power relations among individuals, governments, and corporations. It is a topic of great dimensions involving many social disciplines and domains. Therefore, we will do so by looking at issues such as personal and group privacy, as well as what are appropriate backup systems for digital identity systems based on distributed ledger technology.

A discussion on privacy is significant in that it serves as a proxy for the distinction between the individual and public spheres. This is also something that we highlighted in the section about philosophical perspectives of identity with respect to the constructivist perspective. However, it should be noted that privacy should not merely be regarded as a defensive right. According to the UN's work on privacy in the digital age, this concept has enabling features enabling individuals to express themselves and their perceptions of reality. Although the self-sovereign identity features many elements empowering individuals towards their governments and corporations only final products and practical applications will reveal if these promises are fulfilled.

For instance, when it comes to examining if controllers' obligations could be used for managing Bitcoin according to the EU GDPR legal structure, it is still uncertain whether a collective may act as a controller in the sense of Article 4.7 GDPR or whether its members are joint controllers under Article 26 GDPR.[6] To put it differently, individual rights cannot be asserted if it is not known exactly who is supposed to respect them, protect them, and advance them.

In addition, there is a need to factor in possible tensions regarding issues like the distinction between private and public data, the enforcement of specific individual rights (e.g., amendment, access, erasure of "right to be forgotten", etc.), data protection by design and default as well as other requirements of modern data protection law (Finck, 2018b, p. 26–32). On one hand, advocates of DLT might question the relevance of high standards of data protection for innovative digital identity systems implementation. They view the dataset assumptions on which these are based as out-of-date. On the other hand, they put it rightly when they stand by the fundamental principles captured in the likes of GDPR.

At present, two of the only safeguards against the 'Facebook or Googlization of Everything' (Vaidhyanathan, 2012) are GDPR and international accords like the Convention by the

[6] Biryukova, A.G. & Kolisnykova, H.V. (2024). Civil and legal aspects of digital privacy. *Uzhhorod National University Herald. Series: Law*. 1 (81). p.pp. 173–179. Available from: [Accessed: 5 August 2024].

Council of Europe. This is also more relevant at a time when entire communities do not know that the implementation or use of ubiquitous online technologies undermines their chance for informational self-determination (Taylor et al., 2017, p. 226–234). When digitization is about to set men's identity, such concerns are even more significant.

The other commitment to enabling individual 'self-organized' identity control revolves around social inclusion dimensions and the third tendency triggering demand for advanced digital identities. In developed countries, this is often an unrecognizable problem among individuals but in several parts of the world; however, several people are left out of the social systems because they cannot demonstrate who they are many times. According to a World Bank report in 2018 approximately 1 billion people were facing difficulties proving their identity globally (World Bank Group, 2018, p. 3). This urgent issue was acknowledged by the UN through Sustainable Development Goal (SDG) 16.9 which recognizes the right to legal identity for everyone including birth certificates. But this must be done entirely differently than how national and global identities are managed currently, which will take years if not decades to change. DLT-based digital identities can be an agent of basic changes but we do not know whether countries that are often straining with primary infrastructural needs will be able to jump quickly towards fully decentralized digital identity. However, based on the estimation of the World Economic Forum in late 2018, there will be 150 million blockchain-based identities worldwide by 2022.

NOVEL MECHANISMS FOR DIGITAL IDENTITIES

No matter how much identity becomes digitized, one thing that probably will have to stay rooted in the physical domain is the backup mechanism for DLT-based digital identities. Therefore, if a device comprising self-sovereign identification is lost, stolen, or broken, there should be a means of recovering control over such basic data.[7] Biometrics are currently being argued as possible methods to produce and even recover digital wallets or identity hubs. Although biometrics have the advantage of being more lasting and unsuitable these characteristics have been known to pose a risk when used everywhere.

When a person's biological characteristics are registered, it is possible to create extraordinarily detailed profiles of a person's life and activities. This is often accompanied

[7] Mamun, M.A.A., Alam, S.M.M., Samiruzzaman, M. & Hossain, M.S. (2020). *A Novel Approach to Blockchain-Based Digital Identity System*. In: springer, pp. 93–112. Available from: [Accessed: 10 August 2024].

by completely unintentional results. For example, in 2019, Houthi officials in Yemen were asked by the United Nations World Food Program to allow the implementation of biometric tools like iris scanning and digital fingerprints which would help to monitor suspected fraud during food distribution.[8] Consequently, the aid operations were canceled since the Houthi leaders declined their request citing surveillance concerns over biometric identification systems. The initial demand attracted some ire because critics claimed that it was an excessive response on the part of the UN that also endangered lives that are marginalized Nevertheless, this incident is not the only evidence that the widespread, rampant, and under-examined use of biometrics for identification purposes has adverse effects.

Heavily emphasized use of biometrics lies at the core of the Indian Aadhaar system. On September 26, 2018, the Indian Supreme Court made a landmark ruling that limited private corporations' use of Aadhaar but recognized its reliance on biometric data such as fingerprints or DNA (Indian Supreme Court, 2018). The judges noted that it is up to the government to ensure information security in relation to centralized storage and management of biometric data of over 1.2 billion individuals. The validity of this finding will only be confirmed in the future, without imagining any possibility of misuse by the state itself.

CONCLUSION

Integrating blockchain technology with digital identity verification is the most significant development concerning the intersection of technology and law. Increasingly, it seems that traditional methods are no longer adequate to meet the needs of the digital economy, given their vulnerabilities and inefficiencies. Nevertheless, blockchain provides a solid alternative for such methods because it has an unalterable ledger and operates on decentralized frameworks; thus, making identity management systems more honest and secure.

From a legal standpoint, adopting blockchain-based identity verification calls for existing regulatory frameworks to be reevaluated. Complex issues such as data ownership, movement of information across borders, and legal recognition of decentralized identity must be addressed by jurisdictions. Moreover, in this new norm, all the principles of privacy and data protection set out in different legal instruments including GDPR must be strictly followed.

The role of the legal community is significant in making sure that the application of

[8] Biryukova, A.G. & Kolisnykova, H.V. (2024). Civil and legal aspects of digital privacy. *Uzhhorod National University Herald. Series: Law*. 1 (81). p.pp. 173–179. Available from: [Accessed: 5 August 2024].

blockchain technology conforms to existing laws aside from spurring innovation. Lawyers must find a strategy on how to promote the advantages of blockchain this will enable other lawyers to bring forth how blockchain can help enhance transparency and accountability while dealing with any concerns regarding its use by criminals as it relates to illicit dealings especially online where anonymity prevails A summary of our analysis shows that although blockchain has potential in revolutionizing digital identity verification, there are regulations and laws which need to be followed closely during its rollout process. Therefore it is important for legal experts, technologists as well as policymakers to work together so that this technology can be safe for use; morally right, and assist everybody in society.