Assignment II

Name: Teng Soksereyvathna
Class: C-6 Afternoon
Subject: Blockchain Technology

Write 2 pages: "How immutability protects Digital Identity"

In this era, technology has been implemented in everyone's lifestyle. As it is known for solving people's problems and making lives easier, it also involves the concept of identity which is the digital identity. It is the data stored on computer systems relating to an individual, organization, application, or device and often referred to as a person's online identity. [1] It is constantly under threat from cybercriminals and data breaches because traditional digital records are mutable. The solution to this is immutability, the property of data being unchangeable once written. This helps safeguard digital identities from tampering, fraud, and unauthorized access.

The security offered by immutability comes from its reliance on fundamental cryptographic techniques. Unlike traditional, mutable databases where a record can be simply updated or overwritten, an immutable system relies on cryptographic hashing to link data in a chronological sequence. In systems like blockchain, every new block of identity data receives a unique hash, a fixed-length digital fingerprint, which also incorporates the hash of the previous block [2]. If even a single character in an identity record were altered, the hash would change completely, immediately invalidating the subsequent links in the chain and alerting all parties to the tampering. This makes alteration practically impossible, thereby providing identity security [3].

One of the most common and damaging forms of cybercrime is Identity theft. According to the U.S. Federal Trade Commission, identity theft reports exceeded 1.4 million in 2020 alone [4]. When this data is stored in a central server, it becomes an attractive target for insidious data tampering. Hackers who access these databases can modify or delete identity records, assume someone else’s identity, or create fake credentials. Because traditional systems lack a built-in, cryptographic mechanism to prove the original state of the data, the integrity of a person's digital self has historically been continually at risk, leading to widespread identity fraud and deep mistrust in digital records [5].

Immutability eliminates fraud because credentials like licenses or medical records can't be changed after they're created. This feature is crucial for Self-Sovereign Identity (SSI) models which give people control over their own digital data [6]. For example, when a company checks a digital degree on an immutable ledger, they can trust it because tampering with the record would break its cryptographic signature. This makes digital identity a tamper-evident, verifiable

truth instead of a fragile file that can be easily disputed [7]. Verifiability builds confidence for users and service providers alike. Immutable records enable auditability and traceability, making it easier to confirm when and how identity information was issued or used.

Furthermore, immutability offers big benefits for legal compliance and audits because many global laws like finance regulations require companies to keep detailed, accurate records of how they handle data so immutability is the solution. From a legal perspective, immutability supports compliance with auditing requirements and data protection laws like GDPR and HIPAA which demand strong accountability and data integrity. It automatically creates a complete, chronological, and unchangeable audit trail of every action since each one of them is permanently logged and cryptographically linked [8]. This clear record makes it easy for regulators to verify a company's history of data handling, simplifying legal requirements and making data governance transparent and unbiased [9].

Despite these benefits, immutability creates a conflict with rights like GDPR's "right to be forgotten," which requires data to be deleted upon request. To solve this, new solutions such as emerging off-chain storage keeps sensitive personal information separate and deletable while only on-chain cryptographic proofs are kept immutable [10]. This approach allows users to revoke or delete personal data while the integrity of the critical reference record remains permanently intact.

A permanently unchangeable public record makes physical deletion impossible. Modern identity architects address this challenge through creative solutions that balance security with privacy rather than storing the sensitive personally identifiable information directly on the immutable ledger, developers only store a cryptographic hash or a proof of the data. The actual sensitive data resides in private, encrypted off-chain storage controlled solely by the user [11]. Ultimately, for immutability to serve as a sustainable protector of digital identity, its technical application must be balanced with innovative architectural choices that respect the user's fundamental right to control and remove their personal information.

While immutability helps ensure that digital identity data cannot be tampered with, it also introduces a privacy challenge. If sensitive personal data is permanently recorded on a public blockchain, users may lose the ability to update, hide, or delete that information even if it later becomes irrelevant, embarrassing, or potentially harmful [12]. This creates a conflict with modern privacy standards such as data minimization which states that personal data should only be stored for as long as necessary. To address this issue, digital identity systems should be carefully designed so that only cryptographic proofs or references are stored immutably, while the actual personal data remains off-chain, encrypted, and under the user's control [13]. It balances the benefits of immutability with the need for privacy and flexibility.

In conclusion, immutability is the key to fixing our broken digital identity systems. By using cryptography to make data permanently unchangeable, we eliminate fraud and tampering that plague current centralized databases. This allows for Self-Sovereign Identity (SSI) to give people full control over their credentials. We must use smart designs to respect privacy rights like the "Right to Be Forgotten". The overall advantages are unmatched security, clear audit trails, and better economic efficiency that make immutability the essential foundation for a reliable and trustworthy digital future.

References (IEEE Style)

[1] “Digital identity,” Wikipedia, The Free Encyclopedia, Oct. 2, 2025. [Online]. Available: https://en.wikipedia.org/wiki/Digital_identity

[2] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008. (Self-published paper).

[3] A. Zysman, “The Political Economy of Digital Currencies,” Tech Law Review, vol. 5, no. 1, 2017.

[4] Federal Trade Commission, Consumer Sentinel Network Data Book 2020, Washington, D.C., USA, 2021. [Online]. Available: https://www.ftc.gov

[5] N. Kshetri, “Blockchain’s role in meeting data privacy and security challenges,” J. Bus. Res., vol. 101, pp. 132–142, 2017.

[6] S. Preukschat et al., Self-Sovereign Identity: Decentralised Digital Identity and Blockchain, Tech Press, 2017.

[7] D. Tapscott and A. Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, Penguin, 2016.

[8] S. Hofmann, “Blockchain Technology and the GDPR: The Right to be Forgotten and the Right to Erasure,” Computer Law & Security Review, vol. 33, no. 6, pp. 839-855, 2017.

[9] U.S. Government Accountability Office (GAO), “Report to Congressional Requesters: Blockchain Technology,” GAO-21-396, 2021.

[10] A. Preukschat and D. Reed, Self-Sovereign Identity: Decentralized digital identity and verifiable credentials. Shelter Island, NY, USA: Manning Publications, 2021.

[11] IBM, “Securing digital identity with blockchain and decentralized storage,” White Paper, 2018.

[12] F. A. O. A. F. A. Graglia, P. R. de Campos, and M. I. T. S. K. Aste, “A Decentralized Digital Identity Architecture,” in Proc. Int. Conf. on Blockchain, 2019, pp. 43–52.

[13] M. Dieye et al., “A Self-Sovereign Identity Based on Zero-Knowledge Proof and Blockchain,” IEEE Access, vol. 11, pp. 41103–41117, 2023.