

Digital Identity and Authentication in the Blockchain Era

Bibhu Dash¹, Pawankumar Sharma²

School of Computer and Information Sciences^{1,2}

University of the Cumberland, Williamsburg, KY^{1,2}

bdash6007@ucumberlands.edu¹, psharma8877@ucumberlands.edu²

January 2021

Abstract: In the digital age, our identity is built on our sense of identity, which defines who we are in our families, communities, cultures, and the wider world. The phrase "Know Yourself" (KYS) describes who we are and how we want to be perceived. It covers a range of characteristics, including those related to language, culture, religion, education, character, and career. While these traits help to define our individual identities, in order for governments and institutions to effectively provide services in areas like education, healthcare, banking, employment, and travel, a broader definition of identity is required. As a result, 'Know Your Customer' (KYC) checks are required by regulatory agencies all over the world. These checks are designed to confirm a person's identification before allowing access to services or facilities, such as admission to universities, creating bank accounts, getting loans, receiving health care, getting mobile SIM cards, etc. Therefore, in this digital world, protecting our identities and valuing who we are as individuals should be our first priority. The use of digital identities is becoming more prevalent as paper-based identity verification becomes less common. A greater challenge in the digital age is setting up how to protect our personal information and ensure that we are dealing with the correct individual, which is thoroughly examined in this study.

Keywords:

Digital Identity, Authentication, Blockchain, Data Security, Fraudulent Identities, KYC, KYS

Introduction

A digital identity develops naturally as a result of how personal information is used online and the shadow data that the user's online activities produce. Identity management occurs at both the corporate and individual levels. Companies often gather sensitive user data and keep it along with less sensitive routine business data. The growth of user privacy-centric rules like the General Data Protection Regulation (GDPR) and the shift in the industry focus to corporate IT responsibilities, pose new business risks (Ferdous et al., 2019).

A healthy society and economy depend on a secure identity. We can build healthy societies and international markets when we have a good way to identify ourselves and our possessions (Dash, 2020a). Identity can be defined as a group of assertions about a person, place, or thing. First and last name, date of birth, nationality, address, and some type of national identifier, such as a passport number, social security number (SSN), driver's license number, etc., are typically included in this information for persons (Avellaneda et al., 2019). These informational pieces are generated by centralized organizations (state and federal governments) and kept in centralized databases.

Making sure people and entities are trustworthy and authentic is essential as our lives become ever more intertwined through online platforms and digital transactions. As a tried-and-true method to enable a safe and reliable infrastructure and improve services, blockchain is becoming increasingly popular among governments, businesses, and educational institutions. With its inherent qualities of transparency, immutability, and decentralization, blockchain technology presents a possible solution to the problems associated with identity verification and the creation of digital identities (see Figure 1) (Baars, 2016). An in-depth discussion of the relationship between blockchain technology and identity verification is provided in this essay. Topics covered

include self-sovereign identity, decentralized identity, verifiable credentials, and authentication. The advantages, drawbacks, and possible adoption scenarios are also examined.

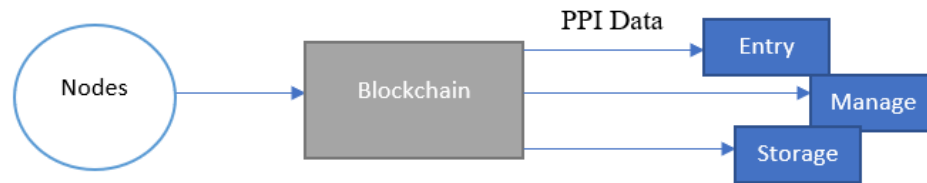


Figure 1. Blockchain on-chain activity of PII data management

Role of Blockchain in Identity Management

Identity management, which includes the identity lifecycle: gathering, storing, and verification of personal data to establish and confirm an individual's identity, is a crucial component of our digital life. Blockchain technology has recently come to light as a potential remedy for identity management, providing a safe and decentralized framework for storing and managing digital identities. Blockchain, the technology that underpins cryptocurrencies like Bitcoin, is a distributed ledger that makes it possible to record transactions across many network nodes. This technology is highly suited for identity management due to its fundamental characteristics of transparency, immutability, and decentralization. Blockchain solves three basic identity management issues in our system: a) Opaqueness b) Data insecurity c) Fake identity (Der et al., 2017).

a) Opaqueness: According to research findings, more than a billion individuals worldwide lack an identity (Unknown, 2020). The majority of them continue to live in abject poverty and never feel the need for identification. The traditional system's hurdles for proper identification are our government's bureaucratic red tape, onerous documentation requirements, and restricted system access. One cannot enroll in school, apply for jobs, obtain a passport, or use numerous government services without having physical identities. To access the current banking system, you must have

an identity. On the other hand, 60% of the 2.7 billion unbanked people already hold a mobile phone, opening the door for mobile identity solutions powered by blockchain that better meet the needs of vulnerable populations (Der et al., 2017).

b) **Data insecurity:** The most important identification data is now kept in centralized government systems that are backed by legacy technologies and have many single points of failure. Hackers are very interested in large, centralized systems that store millions of user accounts' personally identifiable information (PII). According to a 2020 report, 97% of all breaches in 2018 involved personally identifiable information, making it the most frequently targeted data. 2.8 billion consumer data records were exposed in 2018, costing an estimated \$600+ billion, despite regulatory regulations and corporate attempts to improve cybersecurity (Unknown, 2020).

c) **Fake identity:** The user's experience of the digital identification ecosystem is incredibly fragmented. Users switch between multiple identities linked to their usernames on many websites. Furthermore, it is quite simple to manufacture false identities due to the poor connection between online and physical identities. The phenomenon of counterfeit engagement, which can aid in the commission of fraud and result in exaggerated numbers and lost income, thrives in environments where fake identities exist. It is time to create new identity management systems, including digital identity frameworks based on the ideas of decentralized identifiers (DI) and self-sovereign identity (SSI), thanks to the rising sophistication of smartphones, technological advancements in cryptography, and the emergence of blockchain technology (Baars, 2016).

Self-sovereign Identity, Decentralized Identity and Authentication

The self-sovereign identity (SSI) or decentralized identity (DI), in contrast to conventional identity management systems, has emerged as a viable method for addressing the shortcomings of conventional identity management systems by granting complete power to individuals (Know yourself-KYS) (Lundkvist et al., 2017). By giving people complete ownership and control over

their digital identities, SSI enables a paradigm shift by allowing users to manage their identity information and share it with specific individuals only when necessary. Self-sovereign identification systems are made possible by blockchain technology. Individuals can securely and openly store their identity data by taking advantage of the decentralized and unchangeable properties of the blockchain (Avellaneda et al., 2019).

A key element of identity verification in digital identification systems is verifiable credentials (Mühle et al., 2018; Dash, 2020b). They offer a way to prove the legitimacy and authenticity of identity information safely and cryptographically. Verifiable credentials are recordings that attest to characteristics or claims about an individual's identity and are digitally signed and tamper-resistant (see Figure 2) (El Haddouti & El Kettani, 2019). Verifying verifiable credentials includes checking the legitimacy of the issuing authority and the digital signatures using cryptography. Without a centralized authority or middleman, this verification procedure can be carried out by reliant parties, including service providers or organizations. Decentralized identifiers are used to provide individuals with distinctive and globally resolvable identifiers, which further improves the verification process. It gives the highest level of customer confidence and cost savings while avoiding the involvement of several parties and difficult processes.

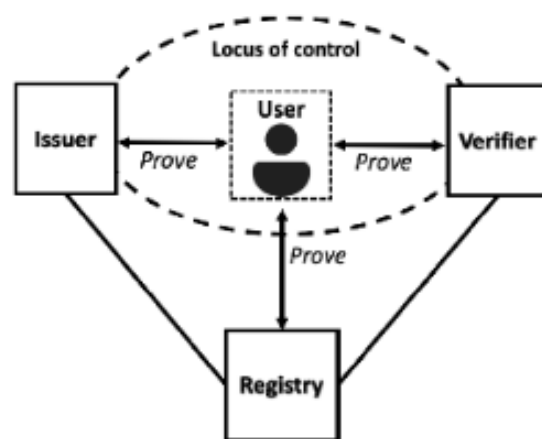


Figure 2. Self-Sovereign Identity using Blockchain.

SSI and Data monetization

As SSI gives data manageability and control back to everyone, people can monetize their accounts in different means without compromising security. Blockchain-based self-sovereign identities and decentralized models give users authority and pave the way for data monetization as the globe starts to consider who should own and benefit from user-generated data. The term "data monetization" describes the use of personal data for measurable financial gain. Even if data has value on its own, the value of the underlying data is significantly increased by insights drawn from personally identifiable data. Each day, 4.39 billion people use the internet, producing a quintillion bytes of data (Lim et al., 2018). By 2022, it's anticipated that more than 60% of the world's GDP will be digital, meaning the value of personal data will continue to rise (Unknown, 2020). For instance, individuals might rent their personal information to businesses, use it to train AI algorithms or sell it to ads. Users would also have the choice to hide and safeguard their data from businesses or governments (Mohammed, 2019).

Benefits and challenges of using blockchain in Identity management.

a) Benefits

There are many benefits to using blockchain technology in data protection, verification, and identity management. The details are outlined below.

Enhanced privacy and control: The idea of self-sovereign identification is one of the main benefits of digital identity solutions. People now have more control over their personal information and can reveal information only when necessary. This improves privacy, lowers the chance of data breaches, and gives people more control over their digital identities (Mudliar et al., 2018).

Supports legal and regulatory outlines: Legal and governmental concerns about responsibility, privacy, and data protection are brought up by digital identity. Blockchain supports

an essential, suitable legislative framework that protects individual rights while striking a balance between compliance, innovation, and security (Mudliar et al., 2018).

High security and trust: Blockchain offers immutability and integrity, making it extremely secure for managing identities. Verifiable credentials that employ cryptographic techniques increase the validity of identifying information, lowering the possibility of fraud and unauthorized access (Baars, 2016).

Speed and cost saving: The necessity for paperwork, manual verification procedures, and reliance on physical papers is eliminated by digital identification solutions, giving high-speed data processing. Identity verification processes are simplified, administrative costs are decreased, and overall efficiency is increased (El Haddouti & El Kettani, 2019).

Interoperability: Verifiable credentials and decentralized IDs are examples of standards that support interoperability and make it possible to integrate identity verification across many systems, sectors, and domains. This makes it easier for enterprises to communicate data in a reliable and effective manner (Dash, 2020c; Ferdous et al., 2019)

b) Challenges

Adoption and Integration Issues: Widespread adoption and integration among numerous stakeholders, including governments, companies, and people, are necessary for the implementation of digital identification systems. It can be difficult to overcome the inertia of current systems, ensure compatibility, and foster consensus among many entities (Mühle et al., 218).

Knowledge gap and technical complexity: Blockchain, self-sovereign identity, and verified credentials are all highly technical concepts involving decentralized networks, cryptographic methods, and compatible data formats. The scalability and performance of these

systems might be hampered by a knowledge gap and subpar technological architecture (Lim et al., 2018).

Government red-taping and legal barriers: Legal and governmental issues like responsibility, privacy, and data protection are brought up by digital identity. It is essential to establish suitable legislative frameworks that protect individual rights while striking a balance between innovation and security (Mohammed, 2019).

Customer experience: The creation of intuitive and user-friendly interfaces for digital identity solutions is crucial for their widespread acceptance. A seamless user experience and the simplification of complex ideas are continuing problems. Wider acceptance and adoption challenges may arise (Avellaneda et al., 2019).

Conclusion

Technology plays a significant role in the disruptive, ever-changing environment of digital identity management. Despite some challenges, blockchain has the potential to change this sector enormously. It can directly impact the financial, healthcare, hospitality, education, and aviation industries to ‘know your customers’ (KYC). The way we identify and manage identities in the digital age is being shaped by identity verification and digital identity. Innovative methods to improve privacy, security, effectiveness, and confidence in identity management systems include blockchain, self-sovereign identification, verified credentials, and authentication techniques. To fully utilize the benefits of these developments, it is necessary to overcome the adoption, integration, scalability, and legal framework concerns. We can build a future where digital identity is frictionless, user-centric, and inclusive, empowering people while fostering a secure and connected digital ecosystem by embracing these technologies and investigating their possible adoption scenarios.

References

1. Avellaneda, O., Bachmann, A., Barbir, A., Brennan, J., Dingle, P., Duffy, K. H., ... & Sporny, M. (2019). Decentralized identity: Where did it come from and where is it going?. *IEEE Communications Standards Magazine*, 3(4), 10-13.
2. Baars, D. S. (2016). Towards self-sovereign identity using blockchain technology (Master's thesis, University of Twente).
3. Dash, B. (2020a). Blockchain Adoption in Enterprises: Opportunities and Challenges.
4. Dash, B. (2020b). Enterprise Risk Management Strategy: SLA, Analytics, and Vendor Lock-in.
5. Dash, B. (2020c). Life on the Edge from Legacy to Cloud Computing: A Case Study on Insurance Industry.
6. Der, U., Jähnichen, S., & Sürmeli, J. (2017). Self-sovereign identity \$-\$ opportunities and challenges for the digital revolution. arXiv preprint arXiv:1712.01767.
7. El Haddouti, S., & El Kettani, M. D. E. C. (2019, April). Analysis of identity management systems using blockchain technology. In 2019 International Conference on Advanced Communication Technologies and Networking (CommNet) (pp. 1-7). IEEE.
8. Ferdous, M. S., Chowdhury, F., & Alassafi, M. O. (2019). In search of self-sovereign identity leveraging blockchain technology. IEEE access, 7, 103059-103079.
9. Lim, S. Y., Fotsing, P. T., Almasri, A., Musa, O., Kiah, M. L. M., Ang, T. F., & Ismail, R. (2018). Blockchain technology the identity management and authentication service disruptor: a survey. *International Journal on Advanced Science, Engineering and Information Technology*, 8(4-2), 1735-1745.
10. Lundkvist, C., Heck, R., Torstensson, J., Mitton, Z., & Sena, M. (2017). Uport: A platform for self-sovereign identity. URL: https://whitepaper.uport.me/uPort_whitepaper_DRAFT20170221.pdf.
11. Mohammed, I. A. (2019). A systematic literature mapping on secure identity management using blockchain technology. *International Journal of Innovations in Engineering Research and Technology*, 6(5), 86-91.
12. Mudliar, K., Parekh, H., & Bhavathankar, P. (2018, February). A comprehensive integration of national identity with blockchain technology. In 2018 International Conference on Communication information and Computing Technology (ICCICT) (pp. 1-6). IEEE.

13. Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. *Computer Science Review*, 30, 80-86.
14. Unknown. (2020). Blockchain for digital identity: Real World blockchain use cases. Consensus. <https://consensus.net/blockchain-use-cases/digital-identity/>

Authors:

Bibhu Dash is a Ph.D. scholar from the School of Computer and Information Sciences at the University of the Cumberlands, KY. His research interests are big data analytics, AI, and Blockchain. This work is part of the course work and doctorate research project he is performing to view *‘the impact the digital era brings to safeguard PII data and identity protection’*.

Pawankumar Sharma is a Ph.D. student from the School of Computer and Information Sciences at the University of the Cumberlands, KY. His research interests are cloud computing, AI, and Blockchain. This work is part of the research project he is performing to view *‘the impact the digital era brings to safeguard PII data and identity protection’*.