American Academic Scientific Research Journal for Engineering, Technology, and Sciences
ISSN (Print) 2313-4410, ISSN (Online) 2313-4402
http://asrjetsjournal.org/

Web 3.0 and its Potential Impact on Privacy Shifting Left in the Development Process

Kiran Sharma Panchangam Nivarthi[a*] , Sudha Balajinaidu[b]

[a]*31108 Algonquin Trail, Chisago City, MN, 55013, USA*
[b]*15251 Pleasant Valley Rd, Center City, MN 55012*
[a]*Email: Kiransnandu@gmail.com*
[b]*Email: sudha1481@gmail.com*

Abstract

The concept of Web 3.0 as the semantic web has been around since the early 2000s, and its decentralized interpretation gained more traction when the term was coined by Ethereum's co-founder Gavin Wood. New programming languages were identified as the first enablers of Web 3.0, but under its new interpretation, other enabling technologies were identified. The three most significant of which are Artificial Intelligence (AI), Machine Learning (ML), and blockchain. IoT is both a concurrent technology and an enabler. Security and privacy-related challenges with the enabler technologies are already being identified and addressed. The privacy challenges associated with Web 3.0 as a whole are more difficult to identify due to multiple reasons, including the nascent form of the technology, the non-standardized definition of Web 3.0, and privacy (And compliance) concerns associated with decentralization. A decentralized version of the internet has the potential to evoke new, unprecedented privacy challenges, some of which may be addressed with further advances in blockchain (a key enabler). Other challenges and trends are associated with the other Web 3.0 enabler, i.e., artificial intelligence. Despite a wide variety of privacy challenges, there is a strong probability that Web 3.0 is highly likely to push privacy left in the development process. Many of the identified challenges with underlying Web 3.0 technologies can be better addressed at the early stages of the development process. Even though we have yet to see how development culture, our approach to privacy, and Web 3.0 as a tech will evolve, especially considering the myriad of new ethical concerns associated with AI, these factors may not impede privacy's shift to the left in Web 3.0.

Keywords: Web 3.0; Shift-left privacy.

---

* Corresponding author.

1. Introduction

The origination of term Web 3.0 is commonly associated with Ethereum's co-founder Gavin Wood who coined the term in 2014 [1]. However, as a natural successor to Web 2.0, Web 3.0 was discussed and researched before 2010 as well. Industry experts and academics had already associated the term with semantic web [2] (web data correctly interpreted by machines), and even now, when advances and Artificial Intelligence (AI) and Machine Learning (ML) are making semantic web into a feasible reality, the term Web 3.0 and the semantic web are often used interchangeably. Early research identified new computer languages as one of the enablers of Web 3.0, which indicates a developer-level interest in the ideation and practical applications for Web 3.0 [3]. The modern interpretation of Web 3.0 (associated with Gavin Wood) focused on decentralized applications (dApps) and building Zero-Trust interaction systems. Its prime goal is control of information and privacy security, i.e., people having complete control of their data, as well as removing intermediaries and achieving true decentralization. Different frameworks and architecture to achieve that have been proposed [4] and may have already moved beyond academia. One method of achieving decentralization and establishing trust without intermediaries is utilizing blockchain, which is emerging as an important enabler of Web 3.0. Challenges associated with blockchain-powered Web 3.0 are already being identified, and the most easily anticipated challenge is resource consumption, for which solutions are presented [5].

The existing literature on Web 3.0 is extensive, and though it's exhaustive in certain areas, others are lagging behind, and the reason is Web 3.0's overlap with other technologies. Some of its enablers, like blockchain, are relatively mature technologies, and even though AI and ML (two other enablers) have come a long way, they are still rapidly evolving. They may transform semantic web applications in unprecedented ways well within the decade. The Internet of Things (IoT) is another potential enabler of Web 3.0, which is expected to erode the boundaries between physical and digital lives even further and is still in its infancy. IoT is expected to trigger more machine-to-machine interactions as well as machine-oriented marketing for smart devices, an avenue that's expected to expedite the maturity of the semantic web. Academic literature on Web 3.0's overlap with these enablers is minimal compared to research resources on its overlap with blockchain.

Security has already been identified as a challenge in Web 3.0 [6] by multiple experts in different contexts. Security solutions, including a variety of privacy computing paradigms/Privacy Enhancing Technologies (PET), are already being considered in the context of the digital economy, addressing security concerns stemming from Web 3.0's overlap with blockchain and cryptocurrency [7]. However, there is limited literature on whether Web 3.0 can impact the security practices in development and shift it left, i.e., deeper into the development side and making security more proactive than reactive.

2. Privacy in Web 3.0

Identifying privacy challenges and current trends in Web 3.0 can help determine if it is already pushing privacy left of the development process or if it has the potential to do so. Privacy and security are strongly interconnected but not interchangeable. However, practices like DevSecOps and pushing security deeper into the development process can pave the way for privacy shifting left as well.

There are certain limitations inherent in the exploration of Web 3.0 (associated literature and research) from a privacy perspective:

- A non-standardized vision of Web 3.0. Different experts have different opinions on Web 3.0, and even tech leaders like Elon Musk [8] with a favorable opinion on crypto consider it a marketing buzzword (for now). This reflects the skepticism in the mainstream tech community.
- The overlap with blockchain technology. The most prevalent interpretation of Web 3.0 melds it with blockchain, where apps and user data reside in blockchain and is governed via consensus, which by extension determines who governs its privacy. It will be difficult to differentiate whether it's the blockchain application development practices pushing privacy left or Web 3.0.
- The lack of standardization and good practices inherent in a decentralized system.
- The potential clash of Web 3.0 and decentralization with regulatory compliance, especially considering the degree of variance in privacy compliance in different regions.

2.1 How Privacy Is Perceived In Web 3.0

Some experts are hopeful about privacy in Web 3.0, as they consider it a significant improvement over Web 2.0, where centralized giants control the flow of personal data and leverage it for profit, something that Web 3.0 will counteract thanks to a decentralized approach [9]. Others are more skeptical. By surrendering more data to Artificial Intelligence (AI), which will be an enabler of Web 3.0 and the personalized experience it promises, there would be different privacy concerns compared to Web 2.0, including data manipulation [10]. This perspective indicates that we may be trading old challenges for new ones. However, since Web 3.0 is still in its infancy, there is a strong probability that these concerns will be addressed before obscuring the potential of Web 3.0, which will require privacy to shift left in the development process. Another negative perspective on privacy in Web 3.0 is associated with Decentralized Financial (DeFi) applications, which are already gaining momentum ahead of Web 3.0 as a whole due to their association with the relatively mature blockchain technology. The perception is that DeFi sites (at least until last year) offer some of the same and some new privacy issues. Third-party trackers used by DeFi apps and architectural weaknesses in DeFi web and mobile apps can lead to privacy concerns like demographic and even financial data (crypto wallet data) being used by a third-party website. One characteristic weak link is the Google Analytics embedding that may be leveraged by malicious entities to connect Ethereum addresses (or other crypto addresses) to real-world identities [11]. There are also concerns regarding how regulatory bodies will balance someone's right to privacy (facilitated by Web 3.0) with financial regulatory practices (like KYC – Know Your Customer) [12].

The same decentralization that promises more privacy to users also diminishes the power of regulatory bodies to enforce privacy rules over the internet due to the lack of intermediaries. The idea is that more individuals/controlling parties in a consensus will take the right measures to ensure privacy across the board. However, this is where privacy shifting left can be a useful practice. Compliance and regulatory bodies can ensure that Web 3.0 applications, even the decentralized ones on the blockchain, meet the requisite privacy requirements.

2.2 Web 3.0 Privacy Challenges

Even though Web 3.0 is touted as a blanket solution to many of the privacy challenges prevalent in Web 2.0, it comes with its own set of privacy challenges. We can gain a better idea of privacy challenges in Web 3.0 by exploring it from two perspectives: Key enabler technologies (AI, blockchain, ML, and Semantic Web), as well as emerging technologies facilitated by or overlapping with Web 3.0 (Ubiquitous Connectivity, Open ID, Open technologies, IoT, etc.) [13].

1. Web 3.0 is more secure against hackers because if they want to control the decentralized network or corrupt the blockchain, they would need to control at least 51% of the nodes [14]. These nodes are devices that might be spread out over a wide geographic area, and each with its own security layers. This starkly contrasts existing networks/servers, where hackers can target the primary server (or multiple servers) to obtain/target every piece of information associated with the network. But fundamental flaws in the code of the blockchain or applications using it and its features (crypto/smart contracts) can result in privacy breaches.

2. Reconciling the privacy and anonymity of the users of decentralized applications built on blockchain in Web 3.0 is a significant challenge. Without the right measures in place, this anonymity can be used by criminal elements.

3. When it comes to the overlap of IoT and privacy, many existing regulations and laws can be considered obsolete. A major overhaul of the existing legal system's interpretation of digital privacy is required in the wake of Web 3.0 [15]. However, changing privacy laws before the technologies have matured is nearly impossible and may inevitably throttle certain IoT technologies from emerging for mainstream adoption.

4. Web 3.0 will be accompanied by a breaking down of silos, and data, which is currently concentrated with few entities, will become more distributed. Even though it will mostly be inaccessible to malicious entities (with the right security measures in place), opening the data to Machine Learning (ML) algorithm might become a common practice with the right Privacy Enhancing Technologies in place. However, the amalgamation of 6G networks and ML in the wake of Web 3.0 might result in unprecedented privacy challenges [16]. The new wealth of data will create new learning opportunities for ML and its ability to identify trends, enhanced Natural Language Processing (NLP), and IoT (which significantly enhances the attack surface/privacy vulnerability) of the individuals, which can be leveraged to attack the privacy of individuals in unique ways.

5. Many IoT challenges and relevant security measures have been identified in existing literature [17]. This includes the challenges associated with mass-produced and deployed IoT sensors [18]. If the security of one of these sensors is compromised, every unit can be considered vulnerable.

These are just some of the challenges associated with Web 3.0 and enabling technologies. These challenges and existing privacy trends can offer insights into how Web 3.0 can push privacy left of the development process.

2.3 Web 3.0 Privacy Trends

Web 3.0 privacy trends can be identified by ascertaining the privacy trends in the three key enabling technologies: Artificial Intelligence (AI), Machine Learning (ML), and Blockchain. These trends (in the context of privacy shifting left) include the following.

- The maturity of AI governance is an idea that shifts privacy left in the development process and deals with concerns like how privacy in new data-fed environments should be governed. And how government and corporate influence over privacy should be managed [19]. It should also be explored from the perspective of AI tools built into larger software packages and suites, challenging to govern separately as part of a digital entity already subject to its own governance practices [20].
- Another trend related to privacy in AI is managing bias [21]. Oversight has to be built into the development process to remove the influence of bias during both AI's learning and execution phases.
- The development and deployment of Machine Learning (ML) algorithms and protocols consider privacy early on in the development and ML training process, starting with the privacy of individuals whose data is being used to train an ML algorithm. It's a major concern in the development of healthcare-related ML algorithms [22]. Threat analysis should also be considered early on in the process to prevent the corruption of training data [23] by malicious entities in order to compromise or gain access to the "clean" datasets, compromising the privacy of the individuals involved.
- For blockchains, the privacy has shifted left for healthcare blockchains/blockchain applications, and privacy attributes are built into the development process early on [24]. Privacy in the blockchain is relatively difficult to tackle from both identity and transaction perspectives, but many potentially impactful solutions are being discussed [25]. Many researchers are looking into hybrid blockchains (with Trusted Execution Environments) for new, experimental privacy-protection avenues [26].
- Privacy concerns are perceived differently by different Web 3.0 enablers. For blockchain, privacy is one of the primary concerns because of decentralization's challenges with privacy. For artificial intelligence, the privacy concerns are more about how it's reshaping how we perceive digital privacy. From a machine learning perspective, privacy concerns are broadened to include machines. For now, the major concern is how to leverage the power of machine learning without compromising data privacy, and it stems from healthcare and financials to less stringent areas of privacy.

3. The Impact Of Web 3.0 On Privacy Shifting Left

Privacy is already a major concern in most Web 3.0 enablers, especially blockchain. Privacy is expected to be a natural consequence of its decentralized nature [27]. Since it's rooted so deep in Web 3.0 core, it's reasonable to expect that it will be addressed early on in the development process. Privacy may also shift left for the development of decentralized and blockchain-based Web 3.0 applications and software, and privacy challenges inherent in the decentralized system may actually be an enabler of privacy shifting left in the development process. The earlier it's addressed, the safer users will feel about using and adopting it.

Privacy is one of the key selling points of Web 3.0, and the sentiment will trickle down to all applications and

software marketed in Web 3.0 space. Another aspect we need to consider is how radically Web 3.0 will penetrate our lives and how it may change user perspectives and preferences when it comes to privacy. We are surrounded by technology in our everyday life now, but they are mostly contained within the scope of certain devices, primarily our phones, and computers. Since we interact with these devices directly, we have an illusion of control over our privacy. We feel like we can control our privacy with proper restrictions and our web interactions. But with smart devices, smart homes, and the growing concept of IoT (concurrent technological advancement avenue and enabler [28]), this perception is getting blurry. Smart homes with devices laced with sensors constantly streaming and processing data can already lead to several privacy issues, and the problem becomes significantly larger if we extrapolate it for a more macro environment – smart cities. Then there are issues inherent in deep learning, which is a core enabler of Web 3.0/semantic web [29].

4. Result

Web 3.0 will have a greater focus on privacy than its previous iteration and but it's difficult to deduce whether its advent will trigger the acceleration of privacy shifting left in the current development culture. However, the current evidence, i.e., literature on Web 3.0 and the research that has been conducted and will be conducted on privacy trends in Web 3.0 enabling technologies (AI, ML, and blockchain), indicate that privacy would be integrated into the development phase in the next iteration of the internet. A wider penetration of DevSecOps practices in the development culture will also augment this.

Privacy will shift left farthest for blockchain development or development that involves blockchain, like AI and ML-augmented tools leveraging blockchain and decentralization. Development focused on other enablers like AI and ML, where most (virtually all) of the data collected and processed will only be viewed by machines/algorithms, will integrate privacy differently. Concerns would include reverse engineering tactics to reveal the privacy of individuals and biased decision-making.

The impact of privacy shifting left in the next iteration of the internet may be strong enough to trigger the formulation of privacy-first frameworks/practices akin to a privacy-oriented version of DevSecOps. It's important to understand that the conclusion that privacy will shift left in Web 3.0 is based on our current interpretation of Web 3.0 and privacy, both of which may shift in the next few years. For Web 3.0, the amalgamation of the semantic web, IoT, AI, ML, and blockchain/decentralized tech may lead to a radically different version of the internet than we have predicted so far. A drastic breakthrough in any of these technologies and humanity's attitude and regulations towards it may lead to a different growth pattern for Web 3.0. As for privacy, a commonplace differentiation in machine-to-machine, machine-to-human, and human-to-human privacy concerns alone can determine how early privacy is addressed in the development process.

5. Discussion

Despite many of its enabler technologies maturing, Web 3.0 (in practice) is still in its infancy. We have yet to see its impact on our daily lives and culture, which will determine how people (users) perceive privacy in Web 3.0 and how their perception is reflected in the development process. The privacy culture may trigger/warrant

certain regulations or regulations that may develop or contribute to a privacy culture in Web 3.0, and these regulations may forcefully shift the privacy left of the development process. There is also the discussion of unprecedented privacy threats associated with advances in AI which may also shift privacy left of the development lifecycle.

Human-to-machine interactions are limited and rudimentary. Until the launch of ChatGPT, were mostly at the level of chatbots, but this may change with more advanced smart devices becoming part of our daily lives. Advanced AI-based tools that can offer advice on legal matters (DoNotPay), financial matters, and health may come with their own privacy and ethical concerns. Commercial entities and governments will have to draw new lines for where an individual's right to privacy is outweighed by public safety concerns. If web 3.0 enables unique interactions with the semantic web and it's sentient enough to draw conclusions from context, like an individual searching for weapons after a traumatic event may lead to a mass shooting, what should the right privacy approach be?

Extensive research is warranted on how different Web 3.0 enablers are influencing privacy-oriented development to gain a clear picture of how much privacy will shift left in the era of Web 3.0.

6. Conclusion

Based on our current understanding of privacy concerns and perception and our understanding of Web 3.0, it's possible to conclude that Web 3.0 will have a strong positive impact on privacy shifting left. However, it's difficult to predict exactly how the culture of privacy will shift with Web 3.0 because of multiple underlying technologies, all with different privacy vulnerabilities and potential solutions. The privacy concerns will evolve as these technologies interact in Web 3.0 and may lead to a privacy-first culture out of necessity, possibly augmented by privacy regulations specific to Web 3.0. Regardless of the catalysts and how Web 3.0 evolves, the privacy expectations of users, and the privacy awareness (and regulations) we have right now, the chances of privacy shifting left are significantly higher than the chances of it remaining on the right.

References

[1] M. Lacity and S. Lupien, "Restoring Trust with Blockchains," in Blockchain Fundamentals for Web 3.0, Epic Books, 2022.

[2] O. Lassila and J. Hendler, "Embracing "Web 3.0"," IEEE Internet Computing, vol. 11, no. 3, pp. 90-93, 2007.

[3] J. Hendler, "Web 3.0 Emerging," IEEE Computers, vol. 42, no. 1, pp. 111-113, 2009.

[4] T. C. Hengjin Cai, "AnArchitecture for Web 3.0 and the Emergence of Spontaneous Time Order," 2022. [Online]. Available: https://doi.org/10.48550/arXiv.2202.10619.

[5] Y. Lin, Z. Gao, H. Du, D. Niyato, J. Kang, R. Deng, and X. S. Shen, "A Unified Blockchain-Semantic Framework for Wireless Edge Intelligence Enabled Web 3.0," 2022. [Online]. Available: https://doi.org/10.48550/arXiv.2210.15130.

[6] R. Rudman and R. Bruwer, "Defining Web 3.0: opportunities and challenges," The Electronic Library,

vol. 34, no. 1, 2016.

[7] C. Chen, L. Zhang, Y. Li, T. Liao, S. Zhao, Z. Zheng, H. Huang and J. Wu, "When Digital Economy Meets Web3.0: Applications and Challenges," IEEE Open Journal of the Computer Society, vol. 3, pp. 233-245, 2022.

[8] S. Mishra and M. A. Srivastava, "WEB 3.0 TECHNOLOGY," International Journal of Research Publication and Reviews, vol. 3, no. 3, pp. 1755-1759, 2022.

[9] A. K. Goel, R. Bakshi, and K. K. Agrawal, "Web 3.0 and Decentralized Applications," in MDPI - 2nd International Conference on Innovative Research in Renewable Energy Technologies (IRRET 2022), West Bengal, India, 2022.

[10] M. R. Bruwer and M. Rudman, "Web 3.0: Governance, Risks and Safeguards," Journal of Applied Business Research, vol. 31, no. 3, pp. 1037-1056, 2015.

[11] P. Winter, A. H. Lorimer, P. Snyder and B. Livshits, "What's in Your Wallet? Privacy and Security Issues in Web 3.0," 2021. [Online]. Available: https://doi.org/10.48550/arXiv.2109.06836.

[12] A. N. Turi, "Currency Under the Web 3.0 Economy," Technologies for Modern Digital Entrepreneurship, pp. 155-186, 2020.

[13] V. Findlay, "Security and Privacy Issues of Web 3.0," Cyber Security and Asset/Information Securitization, 2015.

[14] F. A. Alabdulwahhab, "Web 3.0: The Decentralized Web," in 2018 1st International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 2018.

[15] S. Singh, P. K. Sharma, B. Yoon, M. Shojafar, G. H. Cho and I.-H. Ra, "Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city," Sustainable Cities and Society, vol. 63, 2020.

[16] Y. Sun, J. Liu, J. Wang, Y. Cao, and N. Kato, "When Machine Learning Meets Privacy in 6G: A Survey," IEEE Communications Surveys & Tutorials, vol. 22, no. 4, 2020.

[17] A. Rhayem, M. B. A. Mhiri, and F. Gargouri, "Semantic Web Technologies for the Internet of Things: Systematic Literature Review," Internet Of Things, vol. 11, 2020.

[18] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT Privacy and Security: Challenges and Solutions," Applied Sciences, vol. 10, 2020.

[19] U. Gasser and V. A. Almeida, "A Layered Model for AI Governance," IEEE Internet Computing, vol. 21, no. 6, pp. 58-62, 2017.

[20] "Gartner Identifies Top Five Trends in Privacy Through 2024," 2022. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2022-05-31-gartner-identifies-top-five-trends-in-privacy-through-2024.

[21] D. Roselli, J. Matthews, and N. Talagala, "Managing Bias in AI," in WWW '19: Companion Proceedings of The 2019 World Wide Web Conference, San Francisco; US, 2019.

[22] E. D. Cristofaro, "AnOverview of Privacy in Machine Learning," arXiv: Machine Learning, 2020.

[23] N. Papernot, P. McDaniel, A. Sinha, and M. Wellman, "SoK: Towards the Science of Security and Privacy in Machine Learning," arXiv: Cryptography and Security.

[24] S. Qahtan, K. Yatim, H. Zulzalil, M. H. Osman, A. A. Zaidan, and H. A. Alsattard, "Review of healthcare industry 4.0 application-based blockchain in terms of security and privacy development

attributes: Comprehensive taxonomy, open issues and challenges and recommended solution," Journal of Network and Computer Applications, vol. 209, 2023.

[25] D. Wang, J. Zhao and Y. Wang, "A Survey on Privacy Protection of Blockchain: The Technology and Application," IEEE Access, vol. 8, pp. 108766-108781, 2020.

[26] M. Jones, M. Johnson, M. Shervey, J. T. Dudley and N. Zimmerman, "Privacy-Preserving Methods for Feature Engineering Using Blockchain: Review, Evaluation, and Proof of Concept," Journal of Medical Internet Research, vol. 21, no. 8, 2019.

[27] S. M. Hizam, W. Ahmed, H. Akter, I. Sentosa and M. N. Masrek, "Web 3.0 Adoption Behavior: PLS-SEM and Sentiment Analysis," arXiv, 2022.

[28] G. Hatzivasilis, I. Askoxylakis, G. Alexandris, D. Anicic, A. Bröring, V. Kulkarni, K. Fysarakis and G. Spanoudakis, "The Interoperability of Things: Interoperable solutions as an enabler for IoT and Web 3.0," in 2018 IEEE 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Barcelona, Spain, 2018.

[29] X. Liu, L. Xie, Y. Wang, J. Zou, J. Xiong, Z. Ying, and A. V. Vasilakos, "Privacy and Security Issues in Deep Learning: A Survey," IEEE Access, vol. 9, pp. 4566 - 4593, 2020.