**Understanding Web3 Security**

**What is meant by web3?**

Web3 is the next evolution of the internet, probably utilizing blockchain technologies and tools for decentralization. It is believed that in web3, some believe that an individual will be the owner of the content that is being posted online by them. So, if the post is desired to stay up, it will stay up but if it is desired to be taken down, it can be controlled in web3 because as it is known, when something is on the internet, it is always on the internet. To cite an example, Odyssey is a blockchain alternative to youtube where videos can be posted and creators can earn tokens which are nothing but rewards for viewing.

**What is meant by web3 security?**

Web3 security is nothing but numerous attack vectors that web3 projects and users are made in contact with and the different ways by which they can protect themselves. It can be further defined as a pivotal goal for web3 more precisely and in a broader sense, with the victory of all web3 projects which are dependent on the overall security of the web3 ecosystem.

**What is the difference between web3 and the other web technologies?**

There is a slight difference between web3 and other web technologies. This can be explained in the following manner.

**1.Web1**

This version of web technology is associated with retrieving data on the web without having the chance to interact with it.

**2. Web2**

This version of web technology is mainly associated with contributing data to the web. To cite an example, the example of uploading content can be considered.

**3. Web3**

This version of the web is mainly concerned with both the contribution and the ownership of the data. Individuals can not only contribute data to the web but also own their uploaded data.

**What are some of the biggest Web3 security risks?**

Although Web 3 is a more secure and reliable technology with respect to the other versions, there are a certain number of risks which are associated with web 3 security. The gap that arises in web technologies is a result of their interaction with each other, the way their protocols function, etc. Some of the risks associated are as follows.

1. One of the primary risks of web3 security is their inadequate encryption and verification for API queries. In a general sense, Web3 is an entirely decentralized technology where every node which is connected to the network can communicate with the data stored. But, in reality, there is a dependence on Web3 on Web2 technologies for any type of interaction and other functionalities. Most of the Web3 app front-ends use API queries to the Web3 back-end for different business logic and data storage. But these queries are not digitally signed which makes them risky and vulnerable.

2. Another risk is smart contracts. A study made in 2019 recognized poorly coded Ethereum smart contracts that put approximately $4 million in Ether at the mouth of vulnerability.

3. Another associated risk is the theft of mobile wallets which are primarily cryptocurrency.

**How to mitigate the risks?**

Although there are certain risks concerning Web3 technologies, there are ways in which they can be mitigated. These are as follows.

1. Incorporation of security-by-designs principles is beneficial for web technology.

2. Apart from the existing blockchain models, approaches for different architecture should be incorporated for better security purposes.

3. Appropriate knowledge and proper knowledge of web3 technology must be there.

4. Different types of techniques and methods that prevent attacks on the web must be used.

**References**

1.<https://www.techtarget.com/searchsecurity/tip/7-best-practices-for-Web3-security-risk-mitigation>

2.<https://hackernoon.com/the-best-practices-for-web3-security-risk-mitigation>

3.<https://www.cloudflare.com/learning/insights-web3-security/>

4.<https://securityintelligence.com/articles/dangerous-flaws-web3-according-to-hacker/>

5.<https://www.certik.com/resources/blog/61IYiqqASgw9kA5BsmaqKa-what-is-web3-security>

6.<https://a16z.com/2022/04/23/web3-security-crypto-hack-attack-lessons/>

7.<https://cointelegraph.com/news/future-of-web3-security-with-immunefi-and-brave-ceos-the-bug-house-2022>