### 

### Names of participants:

1. Akash Reddy Jammula

As of today 4/12, I was late I haven’t got any reply from any one from my fellow externs or the team, so I did this task on my own.

### Date and Time:

4/12/24 and 2pm

### Question 1: In your own words (100-150 words), articulate what Webacy does and the utility of its products and services [Discuss for 5-10 minutes]

* Safety Score
* Wallet Watch
* Backup Wallet
* Panic Button
* Crypto Will

|  |
| --- |
| Webacy offers a different products and services designed to enhance safety and security in the digital space.  Safety Score provides users with a comprehensive assessment of their online safety practices, identifying potential vulnerabilities and offering recommendations for improvement.  Wallet Watch is a proactive monitoring tool that alerts users to suspicious activity in their digital wallets, helping to prevent fraud and or unauthorized access.  Backup Wallet ensures that users can securely store and recover their digital assets in the event of loss or theft.  The Panic Button feature allows users to quickly and discreetly signal for help in emergency situations, providing peace of mind and rapid response when needed most from Webacy team. Finally, Crypto Will enables users to designate beneficiaries for their digital assets, ensuring a smooth transition of ownership in the event of unforeseen circumstances like death. Overall, Webacy's products and services empower users to navigate the digital landscape with confidence and peace of mind, safeguarding their valuable assets and personal information. |

### Question 2: How will it help Webacy to know about the up and coming blockchain technologies and the services offered by its competitors? Describe in about 100-150 words, preferably using bullet points [Discuss for 10-15 minutes]

|  |
| --- |
| Knowing about the latest blockchain technologies and services offered by competitors can greatly benefit Webacy in several ways:  Stay Competitive: Understanding competitor offerings allows Webacy to identify gaps in its own product lineup and innovate accordingly, ensuring it remains competitive in the market.  Market Research: Keeping tabs on industry trends and competitor strategies provides valuable market insights that can inform Webacy's product development roadmap and marketing efforts.  Differentiation: By benchmarking against competitors (or having a moat {competitive advantage}), Webacy can highlight its unique selling points and differentiate itself in a crowded marketplace, attracting more customers.  Partnership Opportunities: Awareness of competitor services opens the possibility of strategic partnerships or collaborations that can mutually benefit both parties and enhance Webacy's offerings.  Risk Mitigation: Knowledge of competitor strengths and weaknesses enables Webacy to anticipate market shifts and proactively mitigate risks, ensuring its long-term viability and success.  In summary, staying informed about up-and-coming blockchain technologies and competitor services equips Webacy with the insights and agility needed to thrive in a dynamic and competitive landscape. |

### Question 3: Based on your understanding of web3, blockchain and other related terms, and your experience with cybersecurity for the services you already use, what are some security threats that you know about, or anticipate can happen in the future? Describe in 200-300 words by stating [The threat] [Why it is important to consider]. [Discuss for 15-20 minutes]

|  |
| --- |
| 1. Smart Contract Vulnerabilities: Smart contracts, which are self-executing contracts with the terms of the agreement directly written into code, are/may be susceptible to bugs and vulnerabilities. These vulnerabilities can lead to financial losses, data breaches, or even network disruptions. It's crucial to consider smart contract security because they are integral to many decentralized applications (dApps) and financial transactions on blockchain networks. A vulnerability in a smart contract could result in the loss of funds or compromise the integrity of the application, eroding trust in the underlying blockchain platform.  2. 51% Attacks: In blockchain networks that utilize proof-of-work (PoW) consensus mechanisms, such as Bitcoin and Ethereum, a 51% attack occurs when a single entity or group controls more than half of the network's mining hash rate. This enables them to manipulate transactions, double-spend coins, or even halt network operations. It's important to consider 51% attacks because they undermine the fundamental principles of decentralization and immutability upon which blockchain technology is built. Such attacks can erode trust in the network and destabilize the entire ecosystem, leading to financial losses and reputational damage. I think this is not possible but there may be a chance.  3. Phishing: (or social Engineering) As with any online platform, users in the Web3 space are susceptible to phishing attacks and social engineering tactics. Malicious actors may create fraudulent websites, emails, or social media profiles to deceive users into disclosing sensitive information such as private keys or login credentials. And there is a chance to get the wallet keys by shoulder surfing. It's essential to consider these threats because they can result in unauthorized access to users' wallets or accounts, leading to theft of funds and loss of control over digital assets. Additionally, successful phishing attacks can tarnish the reputation of blockchain projects and hinder mainstream adoption by fostering distrust among users.  In conclusion, understanding and addressing security threats in the Web3 space is paramount to ensuring the integrity, reliability, and trustworthiness of blockchain-based systems and applications. Proactive measures, such as code audits, network monitoring, user education, and adherence to best practices, are essential to mitigating these risks and safeguarding the ecosystem's long-term viability. |

Review your notes and conclude the conversation.