The Cybersecurity Readiness Podcast Series

Episode Title	Using Blockchain Technology to Make Messaging Apps More Secure and Private
Podcast Series	The Cybersecurity Readiness Podcast Series https://www.cybersecurityreadinesspodcast.com/
Host and Producer	Dave Chatterjee, Ph.D. https://dchatte.com
Guest	Kee Jefferys, Technical Co-Founder of Session
Summary Pitch	Dr. Dave Chatterjee and Kee Jefferys, Technical Co-Founder of Session, discuss the use of blockchain technology in enhancing the security and privacy of messaging apps, specifically Session. Session, which has over a million monthly active users, uses a decentralized network of nodes incentivized by Session tokens. Unlike traditional messaging apps, Session does not require a phone number for sign-up and employs onion routing and end-to-end encryption to protect user data. Key emphasizes the importance of considering the threat model and user needs when choosing a messaging app. Session is best suited for high-threat scenarios, while other apps may be more appropriate for regulatory compliance. Session is free, with potential future premium features, and is primarily for individual users.
Action Items and Discussion Highlights	▪ Explore how Session's decentralized network and blockchain-based incentives can enhance security and privacy for messaging apps. ▪ Provide guidance to listeners on factors to consider when selecting a messaging app for their organization, such as threat model, compliance requirements, and user preferences.

	▪ Clarify the differences between email and newer messaging apps in terms of usage patterns and adoption trends in the corporate/enterprise setting. ▪ Explain how Session's design features, such as the lack of user discovery mechanisms, aim to minimize potential misuse of the platform. ▪ Evaluate messaging app options for the organization based on threat model and user requirements. ▪ Consider the pros and cons of using a blockchain-based messaging app like Session versus more traditional options. ▪ Explore integrating Session or a similar decentralized messaging platform if high security and privacy are key priorities.
Time Stamps	00:02 – Introduction 01:54 – Guest's Professional Highlights 03:15 – Motivation for Developing the Session app 05:46 – Overview of Blockchain 07:59 – Using Blockchain to Secure a Messaging app 11:18 – Characteristics of the Session platform 12:17 -- What makes this particular platform very secure and private? One would think that because it's open (Open Source) and because a lot of people are involved in growing it, security and privacy could be an issue. 15:24 – How should organizations evaluate their need for a suitable messaging app? How should organizations go about selecting their messaging app? 19:29 – Types and nature of usage of messaging apps.

	22:40 -- Your messaging app is using Blockchain technology. Is it fair to assume that the blockchain technology is also being embraced by other apps, or is your app fairly unique? 24:56 -- If I were to consider a messaging platform such as Session, can individuals sign up or is it primarily for organizations? 26:13 -- If I sign up with Session and want to communicate with you, you will also have to be part of the Session network, correct? 28:17 – Does it make it difficult for law enforcement to get to the criminals? 32:05 -- If I were to sign up with the Session app, am I paying any kind of subscription fee, or is it free? 32:54 -- If I signed up with Session and decided that I won't use WhatsApp or iPhone messaging, what happens? Am I cut off from people who are trying to reach me using those messaging apps? 36:02 – Closing Thoughts
Memorable Kee Jefferys Quotes/Statements	"In the case of the Session app, instead of having volunteers, we actually provide an incentive to people that are running nodes on the network, and that's in Session tokens." "Actually, the biggest computer in the entire world is Bitcoin." "When you use the Session messaging application, you are using a network of decentralized nodes to store and route your data. So we have the network layer, and then we have the messaging clients themselves, and those are just things that you can download in the app store and use as you would use like Signal or WhatsApp or any of these secure messaging applications. It's just that the back end for us isn't a single

	centralized server like it is in Signal and Telegram. It's a decentralized network of over 2000 nodes." "Session doesn't require a phone number to sign up. Most messaging applications such as Signal and WhatsApp usually require a phone number to sign up, and they may use that as your identity in the network. Phone numbers are pretty insecure. We've seen a lot of SIM swapping attacks in the last two years, and phone numbers weren't built to be secure." "Session uses a decentralized network instead of a single central server or a bunch of central servers. In joining the network, they have to essentially stake a certain amount of tokens, and then they have to follow a certain set of rules. So, it's the same in most of these decentralized protocols like Bitcoin or Ethereum or any of these cryptocurrencies, if you come into the network, you need to follow a certain set of rules, and those rules are enforced by essentially saying, if you don't follow the rules, we're going to take value away from you that you've staked into the network." "We use onion routing network as well. It's similar to Tor, where you bounce your connection through a bunch of different nodes before it hits the final destination. We limit the amount of information that these different nodes in the network get. All of the metadata is encrypted in Session, we use end-to-end encryption, but we also use onion routing to hide the IP address of people that are sending messages on the network." "I think the most important thing to think about when you're trying to decide on a messaging application (for personal or business use) is what is the threat model that you're operating under? Different threat models will determine different messaging applications."

	"Session tends to be for people who are in more high threat scenarios such as the human rights activist, where you're worried about device seizure and you're really don't want to reveal a lot of information about who you are on the network; you want to use end-to-end encryption, and you want to be as private as possible in the network and reduce the metadata that is being used." "I think businesses are still heavily reliant on email for formal communications, communications that need to be audited and tracked; and also for one-to-many communication scenarios. But I think a lot of those one-to-one conversations are moving to tools like Slack MS Teams and for the smaller groups as well, where you need really frequent communication between people." "Session is focused primarily on individuals." "Session doesn't have a native way to be able to discover other users. You need to know their account ID, which is this long alphanumeric string, which you can't guess." We don't run the network that stores those messages. That's run by those decentralized operators all around the world, which store and route messages. So if someone comes to us and asks for messaging content, we actually don't even have access to the encrypted messages. Then, if someone were to ask the decentralized servers for the contents of those messages, because they're end to end encrypted, those intermediaries that relay messages or store messages for a period of time, are unable to share the content. So the only two people that can read a message, is the person who sent it, and then the person who received it. "There's no back doors in Session that would allow you to kind of grab someone's message and give it to a law enforcement agency."

	“Think about the messaging applications that you use and consider what your threat model is, and then just do your own research about what messaging application fits both your threat model and the features you're looking for, what the users actually want to use in your organization.”