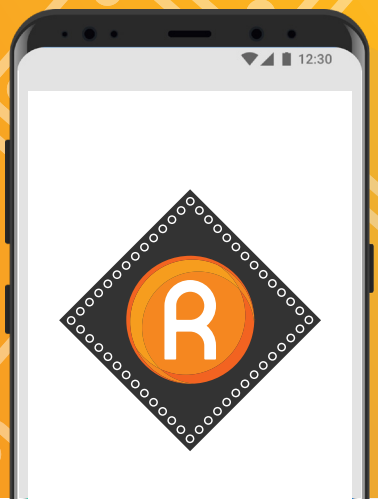
rivetz

Toolkit

Rivetz Network Access
For developers and service providers



Access the Rivetz Network

The Rivetz Toolkit is a collection of software, documentation and support, which allows simple integration with the Rivetz Network ecosystem for mobile, desktop and IoT applications.

Enable the Trusted Execution Environment

The Rivetz Toolkit enables developers to access the Trusted Execution Environment (TEE) for apps. A special combination of hardware, firmware and software is used to create a protected environment for the use and storage of digital assets.

Utilize the Rivetz Attestor

The Rivetz Toolkit enables access to the Rivetz Attestor, which measures, collects and stores via blockchain device health data. Should device health be compromised, Rivetz Attestor denies access to sensitive data.

Why Rivetz?

Rivetz enables simpler and safer multi-factor authentication. Rivetz combines blockchain technology with the hardware-based Trusted Execution Environment (TEE) in mobile devices to deliver decentralized cybersecurity. Rivetz performs a Device Integrity check and validates provable enterprise controls before granting access – delivering a new level of safety and compliance for greater peace of mind.

Trusted Execution

More than one billion mobile devices support the industry standard Trusted Execution Environment (TEE) to provide isolated processing. The TEE leverages isolated storage and execution areas of the processor to protect the user's private keys and enable secure execution of user instructions. Rivetz provides a trusted app that grants access to the TEE in existing mobile devices, enabling this hardware-based functionality.

Key Features

- Blockchain
- Key Transfer & Storage
- Secure Diplay
- Encryption & Decryption
- Attestation

Challenge

In recent Rivetz-commissioned study of 1,000 American adults, more than 50% believe it is the app maker's responsibility to keep their digital information safe. More than one billion devices are equipped with the Trusted Execution Environment (TEE). The problem is, most app developers and service providers don't take advantage of the TEE because it isn't simple to access – developers don't have the tools to utilize it.

The Rivet (RvT)

Then asked whose responsibility it was to keep their data secure, a striking 91% of respondents said they believed the duty was their own – that's where the Rivet (RvT) token comes in. Rivet tokens are purchased as a means to pay for use of the cybersecurity services in the Rivetz Network. RvT tokens are purchased and consumed for all services within the network to deliver endpoint security services and controls on behalf of a service provider or enterprise.

Results

More than 90% of respondents found it important to prevent someone from accessing the content on their smartphone if they lost it. Secure your users' experience – security shouldn't be tacked on, it should be built-in by design. Provide a seamless experience where trust is inherent. Easily develop hardware-based secure applications while working within a familiar Integrated Development Environment (IDE). Create services rooted in strong device identity and secure transactions.