PEERSTREAM PROTOCOL

ENHANCED PRIVATE & SECURE COMMUNICATIONS

For Enterprise and Government Applications

PeerStream Protocol

Privacy Enhanced Data Streaming and Communications

PeerStream Protocol (PSP) is a decentralized binary streaming and routing protocol that is primarily designed to provide real-time data streaming and messaging channels for applications and devices that require the transmission of sensitive data and/or multi-point communications emphasizing enhanced privacy, security features, and control.

PSP is capable of encapsulating different kinds of name-spaced services designed to provide applications with configurable degrees of anonymity, privacy and security, with features including but not limited to end-to-end encryption, user-to-user authentication and metadata termination.

PSP will route live video and data streams leveraging blockchain or inherently decentralized/ distributed P2P networks, offering scalability, security and privacy to the enterprise.

PSP WILL SERVE MULTIPLE TYPES OF APPLICATIONS USED TO GENERATE SECURE LIVE DATA AND CONTENT FOR REAL-TIME DISTRIBUTION:

Consumer Apps:
- social networks
- live video streaming
- video chat

Enterprise Offerings:
- legal / medical comms
- trade secrets / IP
- IoT and sensitive data

Government Solutions:
- interagency channels
- intelligence / military
- foreign ops

PSP OFFERS TWO DIFFERENT LEVELS OF FUNCTIONALITY AND PRIVACY:

- **The first level of functionality** protects user identity along with encypting the data and includes a multimedia video streaming service built on top of a PeerStream proprietary video protocol. The streaming layer is designed to provide low latency and high-quality real-time streaming for social chat and broadcast use cases, though user identities and session content is end-to-end encrypted to support user anonymity.

- **The second level of functionality** provides full anonymity for one-to-one data and video communications and all session management. This layer uses a modified version of The Onion Routing (TOR) protocol (similar to what powers the Dark Web), utilizing a hidden service approach without the need for **exit nodes**, a known security limitation of TOR. Network nodes responsible for streaming the communication are not able to access IP addresses or identities for clients in those sessions. This architecture is ideal for use cases that require the communication of sensitive data.

PEERSTREAM PROTOCOL KEY TAKEAWAYS:

- **PSP Routing:** Unique Routing employed to hide user/client identity and IP (No Exit Nodes)
- **PSP Rendezvous Points:** Disassociating links and metadata between user identities and their IP addresses in all communication and streaming sessions
- **PSP Architecture:** Designed for secured communication channels between crypto-identities in Blockchain networks or more traditionally distributed environments
- **PSP Flexibility:** Configurable to unlock value for demanding live social apps OR for highly sensitive real-time communications and data transmission applications

Contact us : info@PeerStream.com

PEERSTREAM

backchannel

Powered by PEERSTREAM PROTOCOL

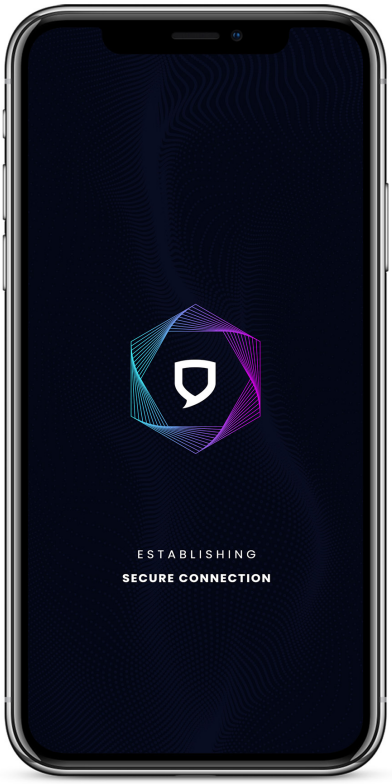
SUITE OF CROSS PLATFORM MIDDLEWARE AND SDKS

Securing the Mobilization of Information for a Range of Applications, Devices and Use-Cases

CASE STUDY: BACKCHANNEL SECURE MOBILE COMMUNICATION SOLUTION POWERED BY PSP

Backchannel is a our branded framework designed for ease-of-use and integration of PeerStream Protocol's capabilities, but it is also the foundation of a best-of-breed secure video-enabled mobile messaging app. Backchannel leverages crypto identity and is able to interoperate with blockchain technologies to provide decentralized messaging and 1:1 live video streaming with exceptional privacy control.

The **Backchannel branded mobile solution** accesses PSP's distributed security model, which uses a variation of The Onion Routing (TOR) protocol implemented so that network nodes can neither trace the origin or destination of messages, nor determine the participating device IP addresses.



Secure communication starts with verified identification of the counterparties, though these parties must be in control of how their identities are used. Backchannel requires **no PII** and can utilize blockchain crypto addresses as user identities. In addition, it will utilize hardware level encryption from the Trusted Execution Environment (TEE) found within most smartphones, providing a level of security and account protection beyond that of leading secure messaging applications available today.

https://www.backchannel.live/

About PEERSTREAM (OTCQB: PEER) PeerStream is a global internet solutions provider pioneering the real-world adoption of emerging blockchain technologies by developing software, services and applications for corporate clients and consumers. PeerStream supports clients' transition to blockchain through license of proprietary software such as PeerStream Protocol ("PSP"), a protocol for decentralized multimedia communications and live video streaming currently in development. PeerStream has a 20-year history of technology innovation and holds 26 patents.

Contact us : info@PeerStream.com

PEERSTREAM