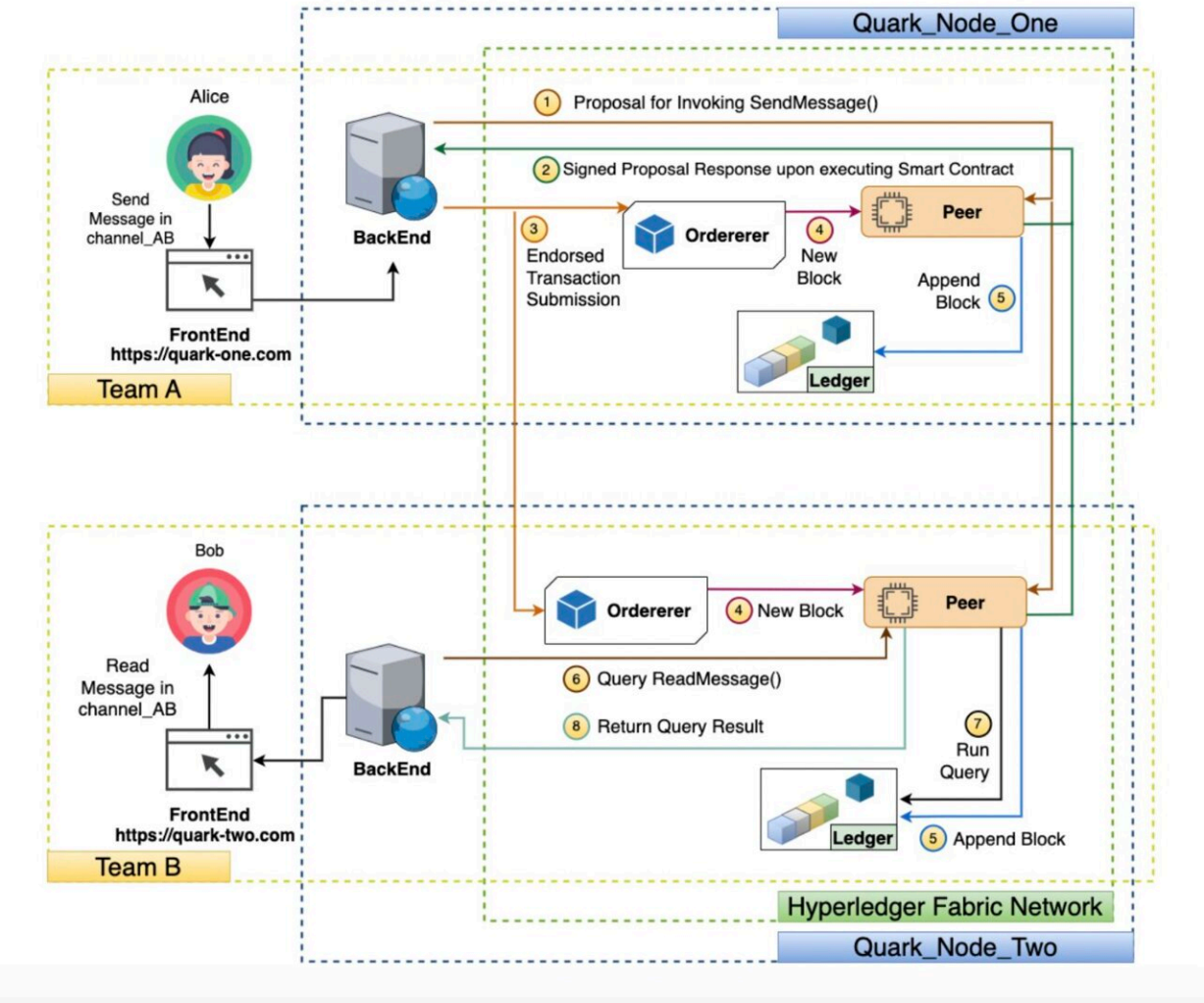


# A decentralized, blockchain-based messaging network for safer communications

August 29 2023, by Ingrid Fadelli



Credit: Shuhan et al

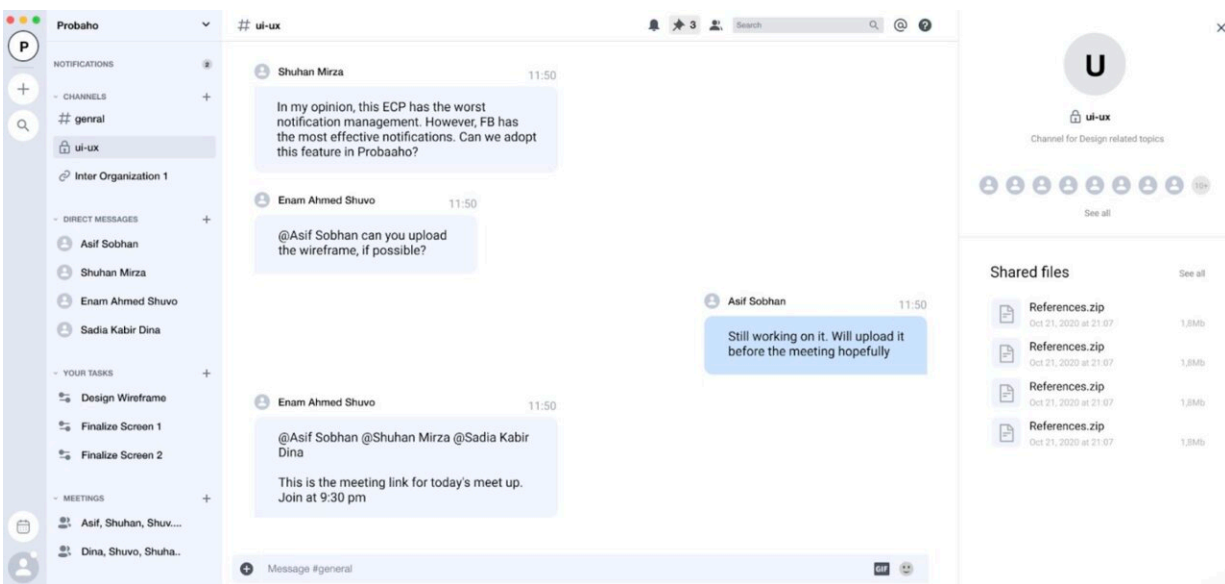
Data and security breaches are becoming increasingly common, highlighting the vulnerabilities of existing messaging and communications platforms. Devising computational tools and systems that better protect sensitive data against malicious attacks is therefore of utmost importance.

With this in mind, researchers at bKash Limited, Syracuse University and other institutes worldwide recently developed Quarks, a new, decentralized messaging network based on blockchain technology. Their proposed system, presented at the [10th IEEE International Conference on Cyber Security and Cloud Computing](#) (CSCloud), and now published in the conference proceedings, could overcome the limitations of most commonly used messaging platforms, allowing users to retain control over their [personal data](#) and other information they share online.

"A few days ago, I came across an article about a [data breach](#) on Discord.io that resulted in the leakage of information of 760,000 users," Shuhan Mirza, one of the researchers who carried out the study, told Tech Xplore. "This kind of incident has become quite common these days and it's hard to trust that messaging companies won't exploit our data. It's also concerning that many governments have attempted to use [instant messaging services](#) against their citizens. That's why we're working on designing a next-generation architecture for instant messaging service based on distributed ledger technology, which will offer us the privacy and reliability we require."

The most notable characteristics of Quarks, the messaging network created by Mirza and his teammates, is that it eliminates what is known as centralized control, essentially preventing third parties, as well as governments and service providers from accessing [user data](#) and messages exchanged on the platform. The Quarks network has two main types of participants, which are referred to as nodes and users.

"To join, a user must create a wallet with a public and private key," Mirza explained. "Afterward, the user must register with a node of their choice using their public key. Once registered, users can create channels and invite others to join. Each channel has a separate ledger hosted by the nodes. Nodes will only host channels that their users are members of. The data in the ledgers are encrypted, and the secret key is managed by the users of the channel."



Credit: Shuhan et al

Notably, in Quarks, every user operation and [information exchange](#) that takes part on a channel is carried out via the ledger's so-called smart contract. In practice, this means that no-one outside of a channel should be able to send or read messages on it. In addition, all messages on the channels cannot be altered or edited, yet they can be audited, meaning that users should be able to derive information about when they were created, sent, delivered, and so on.

As nodes in the Quarks network are distributed across the globe, an attacker would be unable to breach the network and access [sensitive data](#) by targeting a single source or node. This design greatly improves the security of the platform, as it would prevent many of the data breach scenarios that observed over the past few years.

"Our team successfully created a prototype of the decentralized Quarks instant messaging service," Mirza said. "We are optimistic about building a production version of Quarks and believe that enterprises will adopt it as their primary platform for team communication and collaboration. This is because enterprises prioritize the security of their business secrets and Quarks offers a solution that prevents leaks to third parties."

In the future, the blockchain-based messaging [network](#) created by this team of researchers could be deployed worldwide, allowing individuals and enterprises to better secure their communications. Currently, Mirza and his teammates are working on upgrading and perfecting their prototype, to facilitate its large-scale implementation.

"We now want to make our messaging service more scalable and faster," Mirza added. "Furthermore, we are working on a production-ready version of Quarks."

**More information:** Mirza K. B. Shuhan et al, Quarks: A Secure and Decentralized Blockchain-Based Messaging Network, *2023 IEEE 10th International Conference on Cyber Security and Cloud Computing (CSCloud)/2023 IEEE 9th International Conference on Edge Computing and Scalable Cloud (EdgeCom)* (2023). [DOI: 10.1109/CSCloud-EdgeCom58631.2023.00053](https://doi.org/10.1109/CSCloud-EdgeCom58631.2023.00053)

Citation: A decentralized, blockchain-based messaging network for safer communications (2023, August 29) retrieved 27 April 2024 from <https://techxplore.com/news/2023-08-decentralized-blockchain-based-messaging-network-safer.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.