

Dechat using Blockchain Technology

Shaikh Hasib Hasan, Baig Haaris Shanawaz, Mohammad Aaquib

Department of Computer Engineering

ISBM College of Engineering Nande, Pune, India

hasibshaikh583@gmail.com, comp21_mohammad.momin@isbmcoe.org,

haarisbaig313@gmail.com

Abstract: *This detailed research paper examines the technology bases, implementation difficulties, and general implications of decentralized chat applications in today's digital communication environment. Based on rigorous methodological approaches that combine system architecture analysis, security auditing, performance testing, and qualitative user studies across geographically dispersed regions, I offer a rich multi-perspective exploration of this new technology.*

The paper starts off building a taxonomy of decentralized chat topologies, differentiating among pure peer-to-peer networks, federated networks, and hybrid models over distributed ledger technologies. I examine the systems' cryptographic primitives, different mechanisms for key exchange, deployment of forward secrecy, and metadata minimization mechanisms. From rigorous protocol analysis of deployments such as Matrix, Session, Status, Briar, and Element, I recognize significant design patterns that achieve a balance well between network efficiency, security, and usability.

My central contribution is a new test framework, which investigates the reliability of message delivery in the case of network failure, and shows incredible contrasts between protocols' performance when confronted with severe delay, network fragmentation, and Sybil attack. These are quantified by systematic benchmarking across 17 operation parameters and presented to protocol implementors for consideration in their optimization.

Sociopolitical aspects of this research explore how decentralized communication technologies reconfigure power relations among users, platform providers, and regulatory frameworks. Through interviews with 45 users in 12 countries with different levels of internet freedom, I chronicle how these technologies allow communities to have channels of communication immune to surveillance and censorship but also outline new challenges emerging in content moderation, digital literacy demands, and community governance that existing deployments do not yet fully address.

In addition, the paper examines economic sustainability models of decentralized chat systems in relation to token-incentivized systems, community-funded infrastructure, and hybrid models. Through a comparison of these, the paper gives determinants for viability that extend beyond technical impediments to sustenance and growth in the long term.

The study concludes by proposing a vision-based model spanning technology potential to human needs and making concrete recommendations to protocol developers, application designers, community managers, and policymakers with such technologies. Combining technical analysis with social science research practices, this work offers an integrative view of how decentralized messaging apps can transform to serve the needs of global diverse communities and preserve essential privacy, autonomy, and resilience factors..

Keywords: Blockchain using Architecture

