(12) PATENT APPLICATION PUBLICATION

(19) INDIA

(22) Date of filing of Application :12/09/2025

(21) Application No.202541086869 A

(43) Publication Date : 03/10/2025

(54) Title of the invention : Framework for Seamless Cross-Platform Application Synchronization Using Encrypted Blockchain Channels

(51) International classification	:H04L0009400000, H04L0009000000, H04W0004700000, H04L0009320000, G06F0021640000
(31) Priority Document No	:NA
(32) Priority Date	:NA
(33) Name of priority country	:NA
(86) International Application No Filing Date	: :01/01/1900
(87) International Publication No	: NA
(61) Patent of Addition to Application Number Filing Date	:NA :NA
(62) Divisional to Application Number Filing Date	:NA :NA

(71)**Name of Applicant :**
1)Dr. M.Uma Devi
Address of Applicant :Associate Professor, Department of CSE - Data Science, Malla Reddy Engineering College for Women, Maisammaguda,Dhulpet Telangana India Telangana India
2)Dr.T.Gopalakrishnan
3)Mr. Shuvrajit Nath
4)Kandasamy V
5)Dr. M. Rakesh Chowdary
6)Dr Sumit Kumar Rana
7)S Shanthini
8)Deepak Kumar
(72)**Name of Inventor :**
1)Dr. M.Uma Devi
2)Dr.T.Gopalakrishnan
3)Mr. Shuvrajit Nath
4)Kandasamy V
5)Dr. M. Rakesh Chowdary
6)Dr Sumit Kumar Rana
7)S Shanthini
8)Deepak Kumar

(57) Abstract :
Framework for Seamless Cross-Platform Application Synchronization Using Encrypted Blockchain Channels ABSTRACT: This paper presents CrossLink, a decentralized architecture for secure cross-chain smart contract execution that effectively mitigates the inherent limitations of current solutions, which predominantly emphasize asset transfers and depend on potentially vulnerable centralized intermediaries. The large-scale implementation of Internet of Things (IoT) applications, many of which rely on the concept of federation, introduces distinct security challenges stemming from their distributed architecture and the necessity for secure communication among components across various administrative domains. A federation may be established for the duration of a mission, including military operations or Humanitarian Assistance and Disaster Relief (HADR) activities. These missions frequently take place in extremely challenging or hostile conditions, presenting further obstacles to assuring reliability and security. The diversity of devices, protocols, and security requirements across many domains complicates the prerequisites for the secure dissemination of data streams in federated IoT systems. The advent of the integrated metaverse alongside Web 3.0 has merged virtual and physical reality, potentially transforming social networks, healthcare, gaming, and the educational system. Regrettably, this assimilation has revealed avenues for both physical and virtual-reality-generated security concerns, such as avatar impersonation and Sybil attacks. The suggested system demonstrated an increase in successful transactions across all rate controllers during the tests. The impact of the validator count on throughput and latency has been rigorously tested and assessed.

No. of Pages : 8 No. of Claims : 6