Received: 19 July 2023 | Revised: 28 October 2023 | Accepted: 27 November 2023

DOI: 10.1002/cpe.7987

REVIEW ARTICLE

WILEY

The blockchain conundrum: An in-depth examination of challenges, contributing technologies, and alternatives

Iraq Ahmad Reshi | Sahil Sholla

Department of Computer Science and Engineering, Islamic University of Science and Technology, Awantipora, India

Correspondence
Iraq Ahmad Reshi, Department of Computer Science and Engineering, Islamic University of Science and Technology, Awantipora, Kashmir, J&K, India.
Email: rshiraq333@gmail.com

Summary

The accelerated development of information and communication technologies has generated a demand for data storage that is effective, transparent, immutable, and secure. Distributed ledger technology and encryption techniques such as hashing and blockchain technology revolutionised the landscape by meeting these requirements. However, blockchain must overcome obstacles such as low latency, throughput, and scalability for its full potential. Investigating blockchain's structure, types, challenges, promises, and variants is necessary to understand blockchain and its capabilities comprehensively. This paper overviews various aspects, such as emergent blockchain protocols, models, concepts, and trends. We classify blockchain variants into five essential categories, DAG, TDAG, Sharding, Consensus, and Combining methods, based on the structure each follows, and conduct a comparative analysis. In addition, we explore current research tendencies. As technology progresses, it is essential to comprehend the fundamental requirements for blockchain development.

KEYWORDS

blockchain privacy, blockchain review, blockchain scalability, blockchain variants, IoT, smart contracts

1 | INTRODUCTION

Sensitive data transactions usually require an independent third party to operate separately from the communicating nodes. The server provides third-party trust in the client-server model, which handles the responsibility of trust and various communication parameters. However, the censorship of data by governments and large corporations has resulted in a shift from centralized to decentralised technology models. Furthermore, centralizing information on third-party software such as the cloud and other infrastructures compromises user privacy and confidentiality.[1]

With the increasing use of technology, individuals are exposed to additional threats to their human rights, as evidenced by governments' routine curtailment of freedom of expression through online content filtering. The right to privacy in the digital environment has also garnered significant attention in recent years due to the ease with which private data can be accessed. The growth of software like Pegasus,[2] Stuxnet,[3] and Petya[4] in the past few years highlights the problem of data centralisation. The European Union (EU) must link and coordinate control surfaces on human rights and digital policy, according to a report by Reference 5 to ensure that technologies do not negatively impact human rights.

In addition to the issues related to centralized architectures, single-point failures increase the need for a distributed system. While a single system is needed to monitor the entire network, maintaining availability without compromising security parameters is challenging, especially in cases where traffic generation is high. Following the financial crisis of 2008 and the failure of centralized systems, Satoshi Nakamoto published a paper on cash systems using peer-to-peer networks, eventually leading to the development of Bitcoin.[6] The underlying principle of Bitcoin is to

