KOREA MULTIMEDIA SOCIETY KOREA MULTIMEDIA SOCIETY

The 17th International Conference on Multimedia Information Technology and Applications (MITA2021)

July 5 – July 7, 2021
KAL Hotel, Seogwipo, Korea

Certification

Name : Ajay Kumar
Institution : Central University of Himachal Pradesh, India
Title : Blockchain Technology: Challenges & Solution Perspective
Type : Poster Presentation

한국멀티미디어학회인

General Chair
President of the KMMS
Prof. Eung-Joo Lee

Blockchain Technology: Challenges & Solution Perspective

Ajay Kumar[1,2]
Department of Computer Science
and Informatics
ajaykr.bhu@hpcu.ac.in

Yashwant Singh[2]
Department of Computer Science
and IT
yashwant.csit@cujammu.ac.in

Neerendra Kumar[2]
Department of Computer Science
and IT
neerendra.csit@cujammu.ac.in

[1]Central University of Himachal Pradesh, (H.P.) India
[2]Central University of Jammu, J&K, India

***Abstract*— Blockchain is a distributed peer-to-peer (P2P) network infrastructure that is transparent to key stakeholders, extremely secure, and impossible to manipulate any information. The use of blockchain technology is not limited to bitcoin or other digital currency. The goal of blockchain technology is to create a decentralized system that eliminates the need for a mediator. This study provides insights into blockchain technology ideas, development, mechanisms, opportunities, challenges, and relevant solutions based on literature reviews. This study outlines the challenges of using blockchain technology in real-world applications. Finally, suggested recommendations and concluded with future recommendations.**

Keywords— Blockchain technology, distributed ledger, Smart Contracts, Asymmetric Key Cryptography, Consensus model

I. INTRODUCTION

In 2008, the notion of blockchain was suggested, and in 2009, it was deployed (Nakamoto, 2008). Blockchain is decentralized; relying on core ideas includes Asymmetric Key Cryptography enabling digital signatures, Cryptographic Hash Functions, Smart Contracts, and Consensuses like Proof-of-Work and Proof-of-Stake. All signed transactions are recorded in a chain of blocks in the blockchain, which is considered a public ledger. When more blocks are added, it keeps expanding. Because of the blockchain system's decentralization and consensus models must be executed among decentralized nodes to ensure reliability. The goal of blockchain technology is to provide a decentralized approach that overcomes the need for a middleman. A blockchain is a peer-to-peer (P2P) network node. Every node has a copy of the ledger that is identical. We can exchange information without the requirement for an intermediary by using machine consensus to enable (P2P) exchange. Because blockchain technology is based on a consensus model, which means it will run if everyone agrees, it ensures security and integrity [1].

The remaining paper is organized as follows: The literature survey on blockchain is presented in Section 2. In Section 3, opportunities, challenges, and solutions of blockchain are discussed. Finally, Section 4 concluded with future recommendations.

II. LITERATURE SURVEY

In 1991, Stuart Haber and W. Scott Stornetta created the notion of a secured blockchain [2]. Haber, Stornetta, and Dave Bayer enhanced the system in 1992 by including Merkle trees, which enhanced performance by allowing numerous document certificates to be gathered into a single block. In 2008, Satoshi Nakamoto published the first research paper on bitcoin, which described a peer-to-peer (P2P) system for securely transferring money from one point to another. Due to the extreme openness of blockchain technology, it was vulnerable to malicious attacks, resulting in the development of new ways of using blockchain as secure and permissioned networks [1].

A. Blockchain networks can be characterized based on their permission model are Permissionless (Public) and Permissioned (Private) [2].

a) **Permissionless Blockchain:** Anyone can join, read, write and commit blocks, which is similar to the public blockchain. It is hosted on public servers. It has low scalability. It is both anonymous and extremely durable. We can transfer information without the requirement for an intermediary by using machine consensus to enable a point-to-point network. Bitcoin is the world's first permissionless blockchain based on the Proof-of-Work mechanism. Ethereum (ETH) is another popular permissionless type that uses the Proof-of-Stake [3].

b) **Permissioned Blockchain:** Authorized users can join, read and write blocks, which is similar to the private blockchain. It is hosted private server. Permissioned blockchain networks are commonly used to support a particular group of organizations and individuals. It has high scalability. User authentication, access control, and privileges must be met before joining the network. Hyperledger Fabric and MultiChain are all implementing a permissioned blockchain [4].

B. Blockchain Technology: Technologies of blockchain can be divided into four layers described in Table 1.

Table 1: Blockchain Layers

Layer 3	User Interface (e.g. web3)
Layer 2	Applications (DAPPs, Smart Contracts)