Chapter 1
Blockchain–Based Banking:
Theory and Applications

Fasel Qadir
University of Kashmir, Srinagar, India

Gulnawaz Gani
University of Kashmir, Srinagar, India

Zubair Jeelani
(ID) https://orcid.org/0000-0003-4600-2899
Islamic University of Science and Technology, India

ABSTRACT

Blockchain has become the latest buzzword and hottest technology in academics and the IT industry. Blockchain is a decentralized model that maintains data growing at a rapid pace. In 2008, Satoshi Nakamoto has introduced the concept of blockchain. With the development of bitcoin, blockchain concept became popular and is now considered one of the most impactful inventions of the last decade. It has the potential applications in different areas of study such as banks, education, healthcare, internet of things, cryptography, transportation, and so on. It is considered the future of next digital transformation after mainframe computer, personal computer, smart mobiles, and social networking. The main purpose of this chapter is to introduce the concept of blockchain technology, its few important applications in banking industry, and how it can be used to transform financial institutions. Some of the most important applications of blockchain-based banking are payment systems, loans, KYC, and so on.

INTRODUCTION TO BLOCKCHAIN TECHNOLOGY

Making transactions in conventional systems is controlled and managed through third parties rather than directly between two principal activities. To address this issue, the idea and framework of blockchain technology was introduced and has been applied successfully in different application areas such as banking, education, healthcare, and so on. The objective of blockchain technology is to develop decentralized systems where there is no involvement of third party. Its main strengths, such as low-cost, less-time, transparency, security, traceability, data-sharing, data-integrity, etc. makes blockchain an important technology for developing efficient systems. Any attempt to change any block is immutable as the blockchain technology doesn't permit for it because that can be seen by the other members of the technology. So, it makes frauds impossible and at the same time creates trust among the users which further makes the system transparent. These are the reasons that a wide range of applications have been developed underlying blockchain technology (Nakamoto, 2008; Yli-Huumo et al, 2016; Alammary et al, 2019; Ben & Lahami, 2020).

The idea of blockchain is not new. In 1991, two researchers Stuart Haber and W. Scott Stornetta gave the conceptual framework of chain of blocks (Haber & Stornetta, 1990; Haber & Stornetta,1991, Shrimali & Patel, 2021). The idea was to develop a secured system of chain of blocks for timestamping digital documents, so that their forgeries could be stopped. To achieve this target, cryptographic-hash functions and Merkle trees were used to record verified digital documents in blocks. However, the technology became popular only after its use in cryptocurrencies. Bitcoin is one of the most famous examples of cryptocurrencies emerged under blockchain technology and is the first electronic payment system executed without the intervention of intermediaries (Nakamoto, 2008).

One of the main reasons that blockchain technology is so successful today is due to Merkle Trees, also known as hash trees. Merkle Trees are named after Ralph Merkle, who patented them in 1979. In 1992, the concept of Merkle trees were used with chain of blocks for making it more secure. In simple terms, a Merkle Tree or a binary hash-tree is a data structure that is used in blockchain to encode data more efficiently. It consists hashes of other blocks and provides the history of block transactions. Depending upon the block size, it allows each block to hold more than one record. The popular cryptocurrencies such as Bitcoin and Ethereum uses Merkle Trees.

A Proof of Work (PoW) is a consensus algorithm that ensures the transaction success and is responsible for connecting new blocks to the existing chain. However, the computing process takes much time to verify the status of the process but can be checked quickly. Further, tokens of PoW can't be reused because of double-spend problem. So, Hal Finney explored the concept further and solved the double

Related Content

Legal Protection of the Web Page as a Database
Davide Mula and Mirko Luca Lobina (2009). *Database Technologies: Concepts, Methodologies, Tools, and Applications (pp. 2616-2631).*
www.igi-global.com/chapter/legal-protection-web-page-database/8054?camid=4v1a

Knowledge and Object-Oriented Approach for Interoperability of Heterogeneous Information Management Systems
Chin-Wan Chung, Chang-Ryong Kim and Son Dao (1999). *Journal of Database Management (pp. 13-25).*
www.igi-global.com/article/knowledge-object-oriented-approach-interoperability/51219?camid=4v1a

The Effect of User View Characteristics on Database Design Performance of Novices
Dinesh Batra (1997). *Journal of Database Management (pp. 27-36).*
www.igi-global.com/article/effect-user-view-characteristics-database/51182?camid=4v1a

A Measurement Ontology Generalizable for Emerging Domain Applications on the Semantic Web
Henry M. Kim, Arijit Sengupta, Mark S. Fox and Mehmet Dalkilic (2007). *Journal of Database Management (pp. 20-42).*
www.igi-global.com/article/measurement-ontology-generalizable-emerging-domain/3365?camid=4v1a