Chapter 1
Concept of Blockchain Technology and Its Emergence

Padmavathi U.
National Institute of Technology, Puducherry, India

Narendran Rajagopalan
National Institute of Technology, Puducherry, India

ABSTRACT

Blockchain refers to a distributed ledger technology that helps people to regulate and manage their information without any intermediaries. This technology emerges as a promising panacea for authentication and authorization with potential for use in every possible domain including financial, manufacturing, educational institutions, etc. Blockchain has its birth through the concept of Bitcoin, a digital cryptocurrency by Satoshi Nakamoto, called as Blockchain 1.0. Blockchain 2.0 came into existence in 2014 with Ethereum and smart contracts. The challenges such as scalability, interoperability, sustainability, and governance led to the next generation of Blockchain also called as IOTA, a blockchainless cryptocurrency for the internet of things runs on the top of their own ledger called Tangle, which is immune towards quantum computers. This disruptive technology evolved to provide cross chain support and more security through Blockchain 4.0. Finally, the chapter concludes by discussing the various applications of this technology and its advantages and security issues.

DOI: 10.4018/978-1-7998-2414-5.ch001

EMERGENCE OF BLOCKCHAIN

Blockchain, the underlying technology behind cryptocurrencies has its origin that stem from a problem of verifying timestamp digitally in the late 1980s and early 1990s. In 1990, Haber & Stornetta published a paper titled 'How to Timestamp a digital Document'. In this paper, they proposed to create a hash chain by linking the issued timestamps together so that the documents get prevented from being either forward dated or back dated. Later in 1992, the concept of Merkle Trees was added to this design by Haber, Stornetta and Dave Bayer. Merkle trees helped to improve the efficiency of the system by collecting several time-stamped documents into a cryptographically secured chain of blocks. Each record in this chain is connected to the one before it. This helps the newest record to know the history of entire chain. Then, Wei Dai one of the noted researchers, introduced the concept of b-money which is used to create money through solving computational puzzles and decentralized consensus. But this proposal lacks implementation details. (Blockchain, an emerging technology for the future - Data Driven Investor - Medium n.d.)(The Exponential Guide to Blockchain - Singularity University n.d.)(History of blockchain | Technology | ICAEW n.d.)

(A brief history in the evolution of blockchain technology platforms - By n.d.)In 2005, a concept called "Reusable Proof of Work" (RPoW) was introduced by Hal Finney, a cryptographic activist. This concept combined the ideas of both b-money and computationally difficult Hashcash puzzle by Adam Back for the creation of cryptocurrency. RPoW registers the ownership of tokens on a trusted server. These servers allow the users to check the correctness and integrity of users which in turn helps to solve double spending problem. (History of Blockchain | Binance Academy n.d.)

In 2008, a mysterious white paper titled "Bitcoin: A peer to peer Electronic Cash system", by visionary Satoshi Nakamoto gives birth to the concept of Blockchain. In this paper, Nakamoto combined cryptography, computer science and game theory to describe the digital cash "Bitcoin". This helps the participant to transact from one account to another account without the help of intermediaries such as central authority or bank. (A Brief History of Blockchain: Blockchain Basics Book from ConsenSys Academy n.d.) The following timeline table gives a brief explanation on the emergence of blockchain.

Concept of Blockchain

As the world needs more modernization and digitization, everyone is ready to accept and adapt new technologies(Blockchain Technology Explained: Introduction, Meaning, and Applications - By n.d.). Blockchain, a new disruptive technology was