Chapter 60
Blockchain Revolution:
Adaptability in Business World and Challenges in Implementation

Archana Sharma

Institute of Management Studies, Noida, India

Purnima Gupta

Institute of Management Studies, Noida, India

ABSTRACT

As the base of bitcoin, the blockchain has received widespread consideration recently. Blockchain stands for an immutable ledger which permits transactions to occur in a decentralized ways. Applications based on blockchain are numerous for instance financial services, industrial and supply chain services, legal and healthcare services, IoT and blockchain integration, bigdata analytics, and so on. Nevertheless, there are still numerous confronts of blockchain technology like security and fork problems that have to be resolved. This research highlights an inclusive indication on blockchain technology with blockchain architecture in the first phase. And in the second phase, the security challenges and problems associated with blockchain are highlighted. It further proposes and measures up to various typical consensus algorithms used in different blockchains. Research has been concluded with the potential prospects of blockchain as future trends.

INTRODUCTION

In the current scenario, Information Technology has been playing a major role in the development of the financial industry. Financial organizations restructuring the way to interact with each other. However, the well-known practice and standards of this segment may face an all-out revamp as incredible innovations such as Blockchain is a maturing stage.

Blockchain was first described by Stuart Haber in the early nineties. In 2008, Satoshi Nakamoto(Nakamoto S.,2008), introduced the blockchain through Bitcoin as a digital cryptocurrency. Bitcoin as a cryptocurrency based on a network protocol permits the users over the network to execute the transaction with

digital currency or virtual money in a secure manner that must be present only in their systems. As a sequence of blocks, blockchain register and maintain the details of the transaction in a distributed public ledger crossways with various computers that are connected to peer network. A block records every recent transaction as the present component of blockchain and after completion maintained in blockchain as an eternal database. After completion of each block, another block is created. As a technology revolution of Bitcoin, blockchain maintains proof of every transaction over the network as balance and address. The transactions with Bitcoin are entered in sequential order in a blockchain as the bank transactions are maintained. Due to openness, the entire system sustains security as the public property of blockchain. The transaction is transparent and verifies the authenticity of the owner. Blockchain is considered as decentralized architecture without any verification of the transaction by third parties, it creates a serious distraction to the conventional business procedure which requires centralized architecture or verification from a trusted party. The intrinsic properties of blockchain design and architecture are robustness, transparency, auditability, and network security. Blockchain as a distributed database organizes a sequence of ordered blocks and committed blocks are set to be immutable. Due to the immutable property of the committed block, no one can alter it further. The category of blockchain decides the contents of data stored in a block. For example, Bitcoin maintains the transaction details, the amount transferred, the sender, and receiver information. For authentication, an exclusive hash is associated with each block in comparison to a fingerprint. While the creation of the block, the hash is also calculated concurrently, and in case of any alteration in the same block the hash would also be changed. There are mainly three types of blockChain:

Private Blockchain(Permissioned): Access permissions are restricted in private Blockchain. Network administrator's permission is necessary to join like a participant of blockchain or as a validator. Private organizations in general, may function as private blockchain and won't like the public communication on blocks holding perceptive company details.

Public Blockchain(Permissionless): In oppose to private Blockchain, unlimited members of the open internet can join a permissionless blockchain and perform transactions with validations.

Federated Blockchain: It is a fusion of public blockchain and private blockchain. Though Federated blockchain shares alike scalability and privacy accompanied by private blockchain, a major difference is that leader node (a series of nodes), picked in its place of a single unit for transaction verification processes.

In consideration of the application area of blockchain, renowned execution of public blockchain includes Bitcoin, Litecoin, Ethereum, and broadly the majority cryptocurrencies. The foremost advantages are self-sustained network, self-maintenance, and short of infrastructure costs, radically sinking management overheads. Whereas in private blockchains, the major applications are auditing, database management, and normally, performance-based solutions. For open platforms, Multichain may be considered as an example for constructing and arrange private blockchains. In last, federated blockchains are widely employed in the banking, business organizations, and IT sectors. There are various other application areas also where blockchain has been deployed like healthcare, supply chain, legal services.

Even though the characteristics of blockchain technology may convey additional reliable and expedient services, the security issues and challenges behind this innovative technology is also an important topic that is required to concern. The vulnerabilities include endpoint vulnerabilities,public and private key security, vendor risk, lack of standards, and regulation. Blockchain technology is a grouping of a cryptographic algorithm, peer-to-peer communication, mathematic through a consensus algorithm to determine the synchronization difficulty of distributed database. It's a built-in multi-field infrastructure

Related Content

Application of Representation Learning-Based Chronological Modeling for Network Intrusion Detection

Nitin O. Mathur, Chengcheng Li, Bilal Gonenand Kijung Lee (2022). *International Journal of Information Security and Privacy (pp. 1-32).*

www.irma-international.org/article/application-of-representation-learning-based-chronological-modeling-for-network-intrusion-detection/291701

Ethics, Privacy, and the Future of Genetic Information in Healthcare Information Assurance and Security

John A. Springer, Jonathan Beever, Nicolae Morar, Jon E. Spragueand Michael D. Kane (2011). *Information Assurance and Security Ethics in Complex Systems: Interdisciplinary Perspectives (pp. 186-205).*

www.irma-international.org/chapter/ethics-privacy-future-genetic-information/46346

Estimating and Managing Enterprise Project Risk Using Certainty

Scheljert Denas (2017). *International Journal of Risk and Contingency Management (pp. 47-59).*

www.irma-international.org/article/estimating-and-managing-enterprise-project-risk-using-certainty/177840

Survivability of Sensors with Key and Trust Management

Jean-Marc Seigneur, Luminita Moraruand Olivier Powell (2008). *Handbook of Research on Wireless Security (pp. 636-651).*

www.irma-international.org/chapter/survivability-sensors-key-trust-management/22074

Privacy and Security in the Age of Electronic Customer Relationship Management

Nicholas C. Romano Jr.and Jerry Fjermestad (2007). *International Journal of Information Security and Privacy (pp. 65-86).*

www.irma-international.org/article/privacy-security-age-electronic-customer/2457