Hybrid Artificially Intelligent Multi-Layer Blockchain and Bitcoin Cryptology (AI-MLBBC): Anti-Crime-Theft Smart Wall Defense

5

Murad Al Shibli
Abu Dhabi Polytechnic, UAE

INTRODUCTION

This chapter presents an integrated secured framework of blockchain and bitcoin cryptology with the artificial intelligence of neural networks and machine learning. Recently blockchain has been received special attention and used as a new platform for digital information and to store encrypted data and process secure digital transactions. Noticeably, the majority of blockchain cryptocurrency technology is structured based on the elliptic curves digital signature algorithm (ECDSA). In particular, Bitcoin uses special elliptic curves digital signature algorithm (ECDSA) called secp256k1. Losses of personal and organizational data have been reported and occurred due to security breaches of data at minor and major scales using traditional transactional and financial platforms. Furthermore, data on blockchain and Bitcoin platforms are assumed to be highly encrypted and secured state. This feature enable blockchain to be an ideal system to save confidential and personal data as well as sensitive organizational and financial information. Although blockchain and bitcoin databases are encrypted using private keys, but there are many cryptocurrency bitcoin wallets have been reported hacked which resulted in losing millions of dollars. Breaching blockchain can lead to exposing sensitive data to high risk. The artificial intelligent neural networks (AINN) algorithms possess the capability features of processing and operating encrypted data and will lead to minimal risk. Pretrained convolutional neural network (CNN) training is proposed to be implemented a part of the block chain to protect personal data and information as third wall defense against hacking. CCN is used to extract learned image features and use those features to train an image classifier with single pass making advantage of machine learning tools features.

In this chapter presents a literature survey is presented, mathematical background of elliptic curves for real and finite prime fields is introduced, elliptic curves cryptosystem is addressed, and bitcoin digital signatures are demonstrated. Moreover, a novel integrated cryptology approach of artificial intelligence based blockchain and bitcoins by introducing a multilayer security layer and neural networks machine learning and big data mining. Specifically, this revolutionary safe combination criteria is structured by implementing a coupled private key elliptic curves digital signature in order to securely enter into the blockchain and process encrypted data using neural networks. Furtherly, encrypted big data can be processed by neural networks linear regression and out-of-memory tall arrays criteria. Moreover, artificial intelligent machine learning of photography can be encrypted-decrypted by using a pertained Convolutional Neural Networks (CNN) and by utilizing Singular Value Decomposition (SVD) and XOR-Secret cipher key.

DOI: 10.4018/978-1-5225-9715-5.ch075

In this chapter, Section 1 will introduce a literature survey, Elliptic Curves Defined Over Real Field is presented in Section 2, Elliptic Curves Cryptosystem Over Finite Prime Fields is introduced in Section 3, Elliptic Curve Cryptographic Algorithm is addressed in section 4, moreover, Bitcoin Elliptic Digital Signature Cryptosystem is presented in Section 5, Multilayer Elliptic Curve Digital Signatures are introduced in Section 6. Moreover, Protection of Data Using Pretrained Convolutional Neural Network (CNN) and Singular Value Decomposition (SVD) is proposed in Section 7 along with simulations results. Finally, conclusions are drawn in Section 8.

BACKGROUND

In 2008, Bitcoin was introduced for the first time by Satoshi (2008) as a new type of crypto-currency. Bitcoin as a peer-to-peer digital transaction is structured based on non-centralized chain that is not governed by any central financial bank or any government. Nakamoto proposed to use cryptographic transactions to allow any two parties to transact directly with each other without going through the traditional practice of a trusted third party. Due to this new concept and it has been public used worldwide. The mathematical algorithm and transactions of Bitcoins are built based on elliptic curves. An overview of Digital Signature Algorithm (DSA) and its Elliptic Curve Digital Signature Analogue (ECDSA) and related application in the blockchain and Bitcoin technologies are presented in article of Kikwai (2017). To ensure high security levels for users recommended Elliptic Curve Domain Parameters (ECDP) are introduced in the research work reported by Brown doe SEC1 in (2009) and for SEC2 in (2009). The Wireless Application Forum (2001) has developed the wireless transport layer security and associated wireless application protocol WAP-261-WTLS-20010406-a in order to provide privacy, data integrity and secure authentication between two communicating applications. The American National Standards Institute (2001) and (2005) has identified methods to generate and verify digital signature to secure messages and data using ECDSA in two published standards. These curves and parameters are derived based on Elliptic Curve Cryptography regulated by Standards for Efficient Cryptography Group, ANSI and IEEE.

Multiple elliptic curves digital signature algorithm is proposed in research of Bi, Jia & Zheng, (2018). This algorithm will allow selecting many elliptic curves and editing elliptic curve parameters. This scheme is shown to be secure and efficient with two elliptic curves as recommended. Important questions about Bitcoin are addressed in the book published by (Narayanan, Bonneau, Felten, Miller & Goldfeder, 2016). It addresses the principles of Bitcoin, what makes it different, how bitcoins are anonymous, associated applications, regulations, and future trends. An overview of a bitcoin digital transactions is presented in the thesis work of Crossen, S. (2015). Individual transaction details and security, associated blocks as well as Bitcoin public ledger are highlighted along with mathematical Elliptic Curve background. Elliptic Curve Cryptography using the secp256k1 curve, Elliptic Curve Digital Signature Algorithm, and Secure Hash Algorithm 256 (SHA256) are also discussed. Research work reported by (Haddaji, Ouni, Bouaziz & Mtibaa, 2016) addresses the benefits of the implementations of the electronic signature ECDSA compared to the digital signature algorithm (DSA) used to authenticate compressed videos of H.264. The added value of this algorithm is tested on a set of videos to compare strength, add-time, speed, number of gates of some hashed videos using MD5 functions. The research work Ghosh & Nath, (Nov. 2014) presents a theoretical study of data encryption using artificial neural networks (ANN) using Neural Cryptography. Using feedback, ANN is used to produce efficient data encryption systems.