

Prospective Applications of Blockchain and Bitcoin Cryptocurrency Technology

Nasser Taleb

College of Business, Al Ain University of Science and Technology, Al Ain, UAE

Abstract – This paper presents a literature review of Blockchain and Bitcoin technology future applications. Recently Blockchain has received special attention and is used as a new platform for digital information and to store encrypted data and process secure digital transactions. Noticeably, the majority of Blockchain cryptocurrency is structured based on the elliptic curves digital signature algorithm (ECDSA). In particular, Bitcoin uses special ECDSA called secp256k1. Losses of personal and organizational data occurred due to security breaches of data at small and large scales using traditional transactional and financial platforms. Furthermore, data on Blockchain and Bitcoin platforms are assumed to be highly encrypted and in secured state.

Keywords: Blockchain, Bitcoin, Cryptology, Elliptic Curves Digital Signature Algorithm (ECDSA), Digital Signature.

1. Introduction

Blockchain is a type of distributed ledger designed to be managed by a peer-to-peer network transaction generated based on a standardized protocol for communication and validating blocks such that data of a specific block cannot be changed.

DOI: 10.18421/TEM81-06

<https://dx.doi.org/10.18421/TEM81-06>


Corresponding author: Nasser Taleb,
College of Business, Al Ain University of Science and Technology, Al Ain, UAE

Email: nasser.taleb@aau.ac.ae

Received: 19 December 2018.

Accepted: 02 February 2019.

Published: 27 February 2019.

 © 2019 Nasser Taleb; published by UIKTEN. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 3.0 License.

The article is published with Open Access at www.temjournal.com

In 2008, Bitcoin was introduced for the first time by Satoshi Nakamoto as a new type of crypto-currency [1]. 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 it has been publicly used worldwide. The mathematical algorithm and transactions of Bitcoin are also 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 [2]. To ensure high security levels for users recommended Elliptic Curve Domain Parameters (ECDP) are introduced in research work [3],[4],[5],[6],[7]. 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 [8]. 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 [9]. 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 [10]. 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. The benefits of the implementations of the electronic signature ECDSA compared to the digital signature algorithm (DSA) are presented for credentials and authenticated compressed videos of H.264 [11].

Bitcoin systematic analysis of broken primitives are presented in [12]. Cryptographic blocks and related effect on the Bitcoin security are identified. Primitive breakage range of simple privacy violations and full breakdown of the bitcoin currency analysis is revealed. Many findings and recommendations for Bitcoin threat of broken cryptographic primitives are introduced. Unique mistakes and vulnerabilities associated to the implementations of elliptic curve cryptography (ECC), are reviewed and revealed unique in [13]. Bitcoin and other protocols such as secure shell (SSH) and transport layer security (TLS), and Austrian e-ID are studied. It is found that only 10% of the systems support ECC and vulnerabilities are highly exposed.

The concept of Elliptic Curve Digital Signature Algorithm (ECDSA), its mathematical context and successful practice methods are introduced in [14]. ECDSA is considered as asymmetric authentication system which is based on a private key at authenticator level and another public key used at host level to validate the authentication. On the other hand, the symmetric authentication scheme systems used a common secret keys shared by both the user and the host. A new efficient and optimal scheme is proposed to provide a threshold DSA/ECDSA algorithm [15]. This algorithm will enhance the security of Bitcoin wallets to avoid any thefts.

Elliptic Curve Cryptography backgrounded with text and imaged background implementation is briefed in the paper [16]. This is due to the robustness and security of the mathematical compared to other schemes. Prediction of future facts of the Ethereum Blockchain can be explored by Deep Learning (DL) methods reported in [17]. This prediction approach is implemented by using as the transaction count and the account balance distributions. DL is performed to create reusable Blockchain framework to provide data, processing and storage.

This paper is organized as follow: In Section 2 and 3, mathematical background of elliptic curves for real and finite prime fields are presented. Then, in Section 4, elliptic curve cryptographic algorithm is introduced. The author presents in Section 5 and 6 the bitcoin elliptic digital signature cryptosystem and bitcoin digital algorithm. Blockchain strategy is presented in Section 7, with the final conclusion in Section 8.

2. Elliptic Curves Defined Over Real Field

Elliptic curves are defined by cubic equations and are totally different from ellipses or ellipsoids. In a two dimensional plane, the elliptic curve **E** is a cubic curve described over a real domain **R** whose points satisfy the following Weierstrass equation

$$E: y^2 + axy + by = x^3 + cx + d \tag{1}$$

Where x and y take on values in the real number field, and the coefficients a, b, c, d all have real number values. For the purpose of applicability, it is very common to reduce the Elliptic curves introduced in Equation (1) to have the following reduced form

$$E: y^2 = x^3 + ax + b \tag{2}$$

Because the highest order (exponent) is 3, the elliptic curves are said to be cubic equations. Moreover, a zero point is defined with an elliptic curve as a single element denoted O (also called the point at infinity). In order to plot the elliptic associated curve, Equation (2) can be put in the square root form as:

$$y = \sqrt{x^3 + ax + b} \tag{3}$$

For every value of x in Equation (3), negative values of y plot are obtained if specific values of a and b are used. For every quadratic residue x of the elliptic curve defined in (3), there are two solutions existing: y and $-y$. By examining elliptic curves it is found that the associated plots are symmetric about x -axis ($y = 0$). Because of this symmetric property, for every point $P = (x, y)$, there is a negative or inverse negative point $-P = (x, -y)$ such that $P + (-P) = O$. The identity point O can now be added to the elliptic curves group definition such that the group elements can be defined for all points (x, y) on some elliptic curve $= x^3 + ax + b$, and the identity point O . This leads to what is called an infinite group.

Furthermore, the identity point O and all points are located on an elliptic curve form cyclic subgroups.

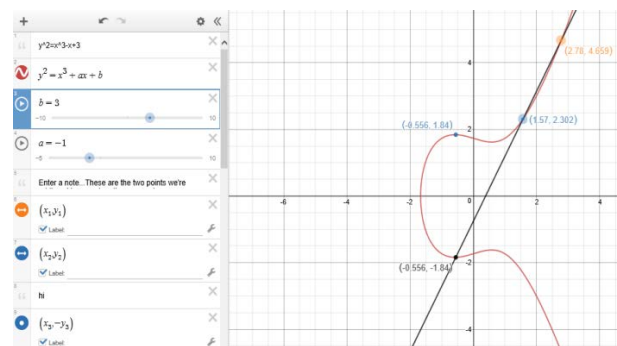


Figure 1: Elliptic Curve Plot over R for: $y^2 = x^3 - x + 3$ ($a = -1, b = 3$)

It is reported that arithmetic operations of elliptic curves over real domains **R** usually lead to irrational numbers and computer truncation errors

and improper memory storage. Therefore, it is recommended to work over finite prime fields associated with elliptic curves. A finite prime field of order q such that $q = p^k$ in which p is a prime and p and k are integers that satisfy the modified original Equation (2) given a domain parameters over \mathbf{F}_q :

$$T = (p, a, b, G, n, h)$$

$$y^2 = x^3 + ax + b \pmod{p} \tag{4}$$

Equation (4) of an integer p identifying the finite prime field \mathbf{F}_q , given that $4a^3 + 27b \neq 0 \pmod{p}$, where p is a large prime. The two coefficients $a, b \in \mathbf{F}_q$, specifying an elliptic curve $E(\mathbf{F}_q)$ defined in Equation (4) with randomly selected elements on $E(\mathbf{F}_q)$ called a base point $G = (x_G, y_G)$. The base point G has an order n which is a large prime that yields $nG = O$ which is defined earlier as the zero element of the field such that $n > 4\sqrt{p}$ and $n > 2^{160}$. The cofactor h is an integer that satisfies $h \neq E(\mathbf{F}_q)/n$. Moreover, the non-singularity condition $4a^3 + 27b$ meant not to be congruent to 0 modulo p .

The elliptic equation described in (2) should satisfy the condition $p \neq 2$. In case that $p = 2$, then Equation (4) will yield to the form:

$$y^2 + xy = x^3 + ax + b \tag{5}$$

Over \mathbf{R} , there is a natural geometric construction that transforms the points of an elliptic curve into an abelian group having O as the neutral element. In this addition of points will be expressed for two points as

follows. The addition for a group operation on $E(\mathbf{F}_q)$ of two points: $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$, an additive third point $P_3 = (x_3, y_3) = P_1 + P_2$

$$x_3 = s^2 - x_1 - x_2 \pmod{p} \tag{6}$$

$$y_3 = s(x_1 - x_3) - y_1 \pmod{p} \tag{7}$$

$$s = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \pmod{p}, & P_1 \neq P_2 \\ \frac{3x_1^2 + a}{2y_1} \pmod{p}, & P_1 = P_2 \end{cases} \tag{8}$$

It is interested to know the total number of points (N) of an elliptic curve given modulo p . It is found that N is almost nearby the prime p as follows:

$$p + 1 - 2\sqrt{p} \leq N \leq p + 1 + 2\sqrt{p} \tag{9}$$

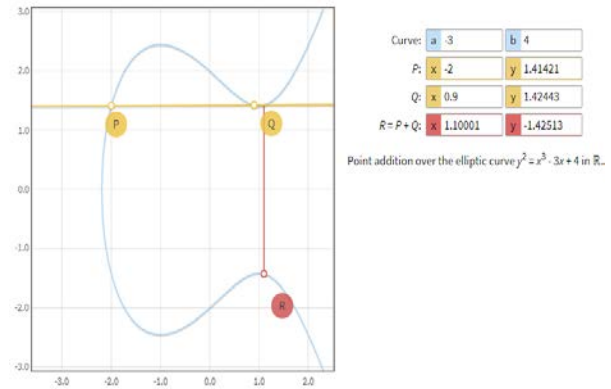


Figure 2: Point Addition Over the Elliptic Curve: $y^2 = x^3 - 3x + 4$ ($a = -3, b = 4$)
Adding two points $P + Q = R = (-2.0, 1.4) + (0.9, 1.4) = (1.1, -1.4)$

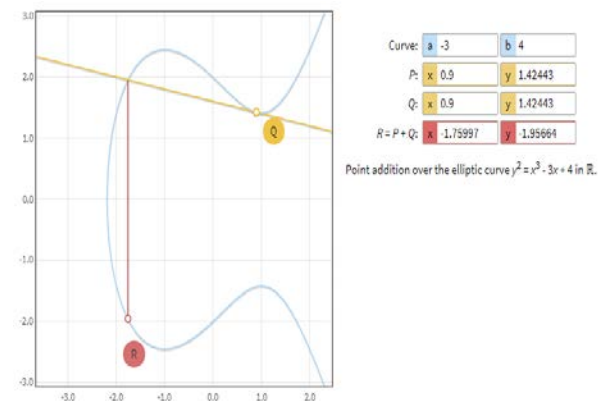


Figure 3: Scalar Multiplication over the Elliptic Curve in Real Field \mathbf{R} for $y^2 = x^3 - 3x + 4$
Doubling a point $A + A = 2 * (0.9, 1.42) = (-1.76, -1.96)$

3. Elliptic Curves Cryptosystem Over Finite Prime Fields

The entire group of an elliptic curve $E(\mathbf{F}_q)$ is not practically needed as a whole, instead a cyclic subgroup is sufficient. A sufficient large cyclic subgroup of $E(\mathbf{F}_q)$ can be generated by selecting the parameters: a, b, p, k and base point $G \in E(\mathbf{F}_q)$. These parameters are shared publicly in Elliptic Curves cryptosystem and used to produce public keys. In general, it is assumed that any point P on the elliptic curve can be generated and expressed in terms of the base point G and a non-negative integer n as follows:

$$P = G + G + \dots + G = nG \tag{10}$$

Based on the Equation (10), it is easy to calculate the new point P provided a base point G and an integer n . But on the other hand, it is very hard and infeasible to do the opposite and find the integer n given the point $P = nG$. Furthermore, double and

add scheme is defined for an elliptic curve group element P and n is an integer, then $n \cdot P$ is a multiple copies of the base point P added together using point addition.

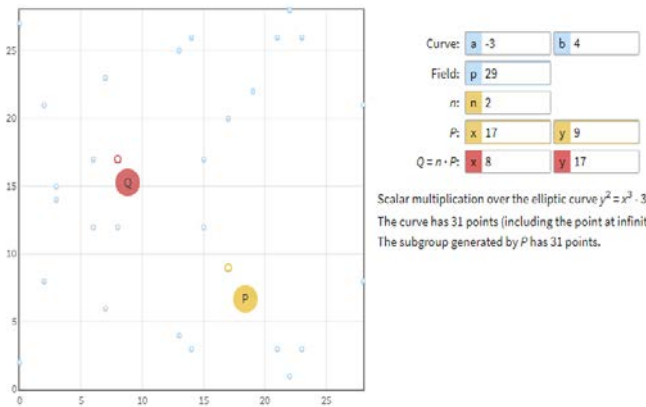


Figure 4: Doubling a Point of an Elliptic Curve in Finite Prime Field $F: y^2 = x^3 - 3x + 4$
 Doubling a point $P + P = Q = 2 * (17, 9) = (8, 17)$

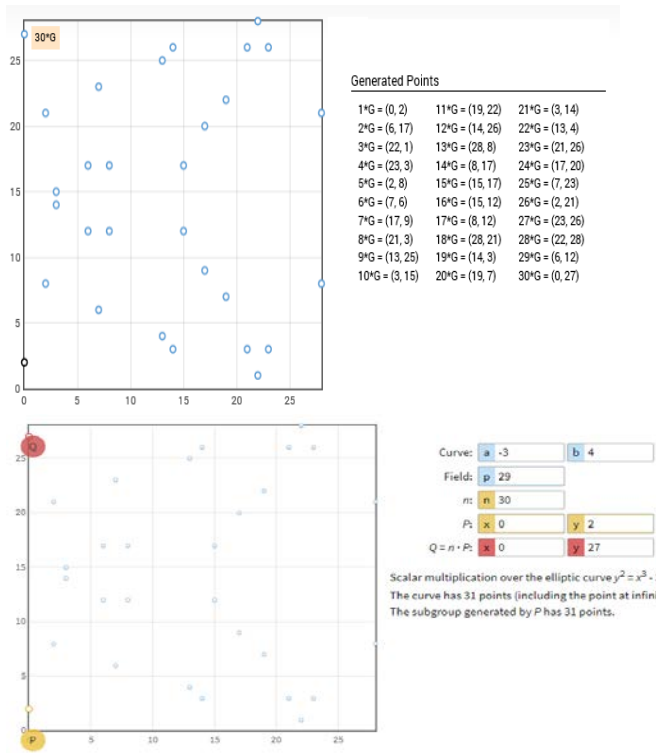


Figure 5: Multiples of the Base Point $P(0, 2.0)$ over the Prime Field: $y^2 = x^3 - 3x + 4$ with Modulus 29

4. Elliptic Curve Cryptographic Algorithm

In order to perform a successful and secure elliptic curve cryptographic algorithm, the following parameters are required:

1. A finite elliptic cubic curve coefficients a and b ;
2. A finite prime modulus p ;
3. A base point $G = (x, y)$ with which point multiplication will be performed such that $n \cdot P = O$. The order of G is identified by the value n . It should be noted that n must be a large prime number. The size of n determines the level of the security.

Hash Function: Hash function H is very important to create and verify a digital signature. It is defined as an effective computational function that needed to map a random length binary string to a fixed length binary string. Hash function H should meet the following technical specifications:

1. **Collision Resistance:** An infeasible computational condition to find two distinct inputs r_1 and r_1 such that $H(r_1) = H(r_2)$;
2. **First Pre-Image Resistance:** For any given output z it is not feasible to find an input such that $H(r) = z$.
3. **Second Pre-Image Resistance:** An infeasible computational condition for a given input message r to another inputs r' such that $H(r) = H(r')$;

This is crucially important for digital signatures as primitive cryptographic that is based on authentications, authorization and non-rejection.

5. Bitcoin Elliptic Digital Signature Cryptosystem

The Bitcoin invented by Satoshi Nakamoto is defined over a finite prime field of order q such that $q = p^k$ in which p is a prime and p and k are integers that satisfy the Equation (2) given a domain parameters over $F_q: T = (p, a, b, G, n, h)$

$$y^2 = x^3 + 7 \pmod{p} \tag{11}$$

Figure 6. demonstrates the plot of the Bitcoin Elliptic Curve over $R: y^2 = x^3 + 7$ ($a = 0, b = 7$). On the other hand, plotting Bitcoin Finite Prime Field to display addition of points with a given modulus is shown in Figure 7.

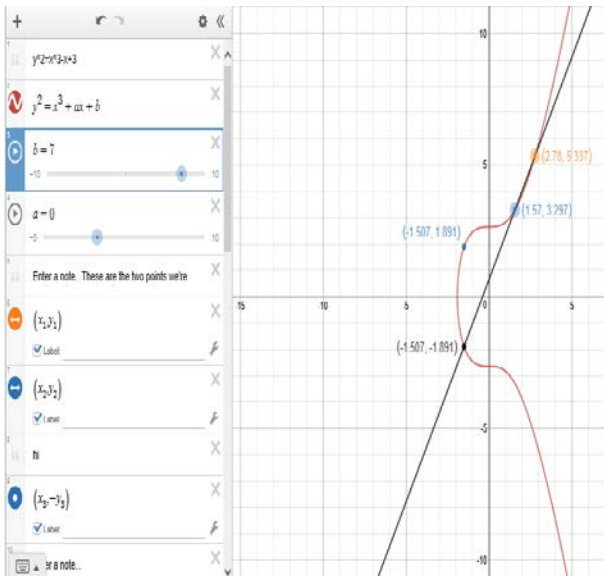


Figure 6: Bitcoin Elliptic Curve Plot over $R: y^2 = x^3 + 7$ ($a = 0, b = 7$)

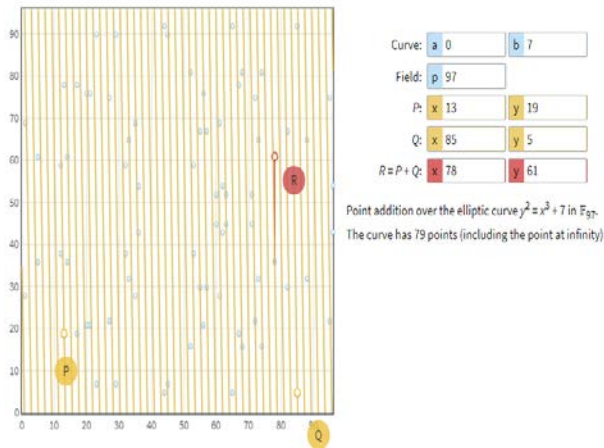


Figure 7: Bitcoin Point Addition over the Finite Prime Field for $y^2 = x^3 + 7 \pmod{97}$
Adding Points $P(13, 19) + Q(85, 5) = R(78, 61)$

6. Bitcoin Digital Algorithm

Define an elliptic curves digital signature algorithm (ECDSA) such that: $y^2 = x^3 + 7 \pmod{p}$.

A signer selects a random number $m \in [1, n]$ as a private key and calculate a public key $Q = mG$

Phase 1: ECDSA Signature Generation: An initiator sends a message M as follows:

Step 1: Compute a secure hash H such that $e = H(M)$;

Step 2: Choose a random cryptographic integer k from the range $[1, n - 1]$ and then calculate $kP = (x, y)$;

Step 3: Calculate r such that $r = x \pmod{n}$ and not to be zero. If zero, then go back to step 2.

Step 4: Compute $s = k^{-1}(e + mr) \pmod{n}$;

Output: The cryptographic signature is (r, s) .

Phase 2: ECDSA Signature Verification: A receiver can check if the message M is true as follows:

Step 1: Check that r and s are integers in $[1, n - 1]$, if not then the signature is not valid.

Step 2: Calculate the hash H such that $e = H(M)$ as in phase 1.

Step 3: Determine w as $w = s^{-1} \pmod{n}$;

Step 4: Compute $u = ew \pmod{n}$ and $v = rw \pmod{n}$;

Step 5: Obtain $R = uP + vQ = (x, y)$;

Output: The signature is valid if only if $r = x \pmod{n}$. Otherwise it is not valid.

The modulus, base point, public key and private keys are demonstrated in Figure 8. and 9. of Bitcoin digital signature.

ECDSA Signature:

secp256k1 (Bitcoin): $y^2 = x^3 + 7 \pmod{p}$.

$P = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^5 - 2^4 - 1$;

$P = 11579208923731619542357098500868790785$
 $3269984665640564039457584007908$
 834671663

$x = 0x79BE667EF9DCBBAC55A06295CE870B0$
 $7029BFCDB2DCE28D959F2815B16F81798$

$G_y = 0x483ADA7726A3C4655DA4FBFC0E1108A8$
 $FD17B448A68554199C47D08FFB10D4B8$

Public Key:

$x: 398746177766303278131900584138165607677$
 $34954098998567043224950074533143699292$
 $y: 83115399533222200534442050051826386603242$
 $609920409430626876080623730665355556$

Signature:

$r: 25282362915497655056329512917121654088602$
 $539327808216077267936411779996643728$
 $s: 39257440409490934652644589859771879805788$
 $241064351461738307073788061051966857$

- Saving working hours
- Saving million printed documents
- Saving money in transactions
- Ensuring the digital security of documents and transactions

The adoption of Blockchain is based on the following features:

- Data and information cannot be hacked or altered;
- Operational cost will be reduced;
- Decision-making will be accelerated;
- Each customer will be given an ID number needed to access their data on the secure chain.
- Digital signature within a permissioned network with known identities.
- Each block is time stamped and encrypted which can be edited by the owner through a private key that only they have
- An individual block, everyone's distributed Blockchain is updated and synced in real time.

The Blockchain as a shared immutable real-time ledger will be used for

- Recording the history of financial transactions
- Contracts
- Physical assets
- Supply Chain information
- Non-centralized operations
- Transferring Accounts within UAE banks
- Controlling Invoices for Business
- Lease and Mortgage Contracts
- Cheques Records
- Loans

8. Conclusion

In this study, an overview of Blockchain and Bitcoin technology is presented along with prospective and future applications. Recently Blockchain has received special attention due to its encrypted data and secure digital of peer-to-peer transactions. The implementation of Blockchain has a promising future represented in: saving working hours, saving million printed documents, saving money in transactions, and ensuring the digital security of documents and transactions.

This new innovative technology has its own advantages and disadvantages that receives some support as well as some concerns. First, advantages of the Blockchain Technology are summarized as follow:

- Zero Percentage of Fraud
- Non-centralized Process
- Instant Transactions
- Improved Financial Efficiency

Second, the disadvantages of the Blockchain Technology are summarized as follow:

- Digital black market
- Non-Tangible and Extremely Volatile
- High tech for Traditional Customers or Operations

References

- [1]. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. UNICAMP –IA368.
- [2]. Kikwai, B., (2017). Elliptic Curve Digital Signatures and Their Application in the Bitcoin Crypto-currency Transactions, *International Journal of Scientific and Research Publications*, 7(11).
- [3]. Brown, D., (2010). SEC 2: Recommended Elliptic Curve Domain Parameters, Standards for Efficient Cryptography, Certicom Research, Version 2.0.

- [4]. Standards for Efficient Cryptography Group, (2009). SEC 1: Elliptic Curve Cryptography, Version 2.0.
- [5]. Wireless Application Forum. WAP WTLS: Wireless Application Protocol Wireless Transport Layer Security Specification, (1999).
- [6]. American Bankers Association. Public key cryptography for the financial services industry: The elliptic curve digital signature algorithm (ecdsa). *ANSI X9*, 62-1998.
- [7]. ANSI, X. (1998). 63: Public Key Cryptography for the Financial Services Industry, Key Agreement and Key Transport Using Elliptic Curve Cryptography. *American National Standards Institute*.
- [8]. Bi, W., Jia, X., & Zheng, M. (2018). A Secure Multiple Elliptic Curves Digital Signature Algorithm for Blockchain. *arXiv preprint arXiv:1808.02988*.
- [9]. Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press.
- [10]. Crossen, S., (2015). The Mathematics of Bitcoin, Master Thesis, Department of Mathematics Emporia State University.
- [11]. Haddaji, R., Bouaziz, S., Ouni, R., & Mtibaa, A. (2016). Comparison of Digital Signature Algorithm and Authentication Schemes for H. 264 Compressed Video. *International Journal of Advanced Computer Science and Applications*, 7(9), 357-363.
- [12]. Giechaskiel, I., Cremers, C., & Rasmussen, K. B. (2016). On Bitcoin Security in the Presence of Broken Crypto Primitives. *IACR Cryptology ePrint Archive*, 2016, 167.
- [13]. Bos, J. W., Halderman, J. A., Heninger, N., Moore, J., Naehrig, M., & Wustrow, E. (2014, March). Elliptic curve cryptography in practice. In *International Conference on Financial Cryptography and Data Security* (pp. 157-175). Springer, Berlin, Heidelberg.
- [14]. Linke, B., (2014). The Fundamentals of an ECDSA Authentication System, Tutorial Article, Maxim Integrated.
- [15]. Gennaro, R., Goldfeder, S., & Narayanan, A. (2016, June). Threshold-optimal DSA/ECDSA signatures and an application to Bitcoin wallet security. In *International Conference on Applied Cryptography and Network Security* (pp. 156-174). Springer, Cham.
- [16]. Kolhekar, M., & Jadhav, A. (2011). Implementation of elliptic curve cryptography on text and image. *International Journal of Enterprise Computing and Business Systems*, 1(2).
- [17]. Besarabov, Z., & Kolev, T. (2018). Predicting digital asset market based on blockchain activity data. *arXiv preprint arXiv:1810.06696*.