Available online at www.worldscientificnews.com

World Scientific News

An International Scientific Journal

WSN 113 (2018) 31-36 EISSN 2392-2192

Cryptocurrency - A Mathematical Extravaganza

Ruchira Goel

Department of Applied Science & Humanities, Ajay Kumar Garg Engineering College, Ghaziabad - 201009, U.P. India

E-mail address: ruchira2002@gmail.com

ABSTRACT

Paper emphasizes some aspects of Cryptocurrency which has evolved in the digital era with elements of mathematical theory and computer science to become a way to secure communications, information and money online. It also addresses a major issue regarding the existence of one of the most prevalent form of Cryptocurrency prevalent these days known as "Bitcoin". Bitcoin don't actually exist but are digital keys that are stored in a digital wallet which exist either in the cloud or on computers and can be linked to bank accounts.

***Keywords*:** Cryptocurrency, Bitcoin, Elliptic Curve Cryptography

1. INTRODUCTION

A cryptocurrency is a digital or virtual currency that uses cryptography –a form of secret coding originating from the Second World War. It is difficult to counterfeit because of this security feature. It uses encryption techniques to control creation of monetary units and to verify the transfer of funds. Hence it is very secure. It has no physical form and is not redeemable in another commodity like gold. Its supply is not determined by any central bank or authority and the network is completely decentralised. Bitcoin, Litecoin, Namecoin and PPcoin are examples of cryptocurrencies. There has been a proliferation of cryptocurrencies in the past decade and there are now more than 1000 available on the internet. The first cryptocurrency is Bitcoin

(Received 02 October 2018; Accepted 23 October 2018; Date of Publication 25 October 2018)

which was created in 2009 by an unknown person using alias Satoshi Nakamoto and is still the best known. The "coins" are made by computers solving a set of complex maths problems.

2. MATHEMATICS BEHIND BITCOINS

To ensure that transactions involving Bitcoin are secure something called 'Elliptic curve Cryptography' is used between owners of Bitcoins. Elliptic curve Cryptography is a type of public key cryptography, relying on mathematics to ensure that a transaction can be secure. Elliptic curves are a very important new area of mathematics which has been greatly explored over the past few decades [2]. They have shown tremendous potential as a tool for solving complicated number problems and also for use in cryptography [5-7].

Elliptic curve cryptography, just as RSA cryptography, is an example of public key cryptography. The basic idea behind this is that of a padlock. In public key cryptography messages are encrypted using particular pieces of mathematical information, which constitute the public key — that's the open padlock and performing the encryption is like snapping the padlock shut. If a secret message has to be too sent to Mr. Y by Mr. X then Mr X will ask to send him an open padlock to which only Mr Y has key. Mr. X then put his message in a box, lock it with the padlock, and send it to Mr. Y. The good thing about this approach is that the message can be sent over insecure channels — even if someone intercepts the box, they don't have the key — and that both of them don't need a key to the box. One could even get lots of people to send someone secret messages in this way, without ever having to give away a single key. Decryption is only possible using a mathematical private key, which is next to impossible to determine if you only know the public key.

In RSA cryptography the public key involves a natural number N, which is used by computers to encrypt messages. To decrypt a message, one need to know the factors of N. If N is very large, then factoring it takes such a large amount of computing power that breaking the code is practically impossible. Only people (or, realistically, computers) in possession of the private key (the factors of N) can decrypt the message easily.

In 1994 one of the most famous mathematics' problems of the last 400 years, Fermat's Last Theorem, was solved by Andrew Wiles, together with his former student Richard Taylor, using elliptic curves. A lot of research has been witnessed in the last few decades resulting into using elliptic curves instead of RSA encryption to keep data transfer safe online.

3. ELLIPTIC CURVES

Elliptic curve cryptography is based on the difficulty of solving number problems involving elliptic curves. On a simple level, these can be regarded as curves given by equations of the form

$$y^2 = x^3 + ax + b$$

where a and b are constants [1]. Below are some examples. In each case (Fig. 1) shows all the points with coordinates (x, y), where x and y satisfy an equation of the form shown above.

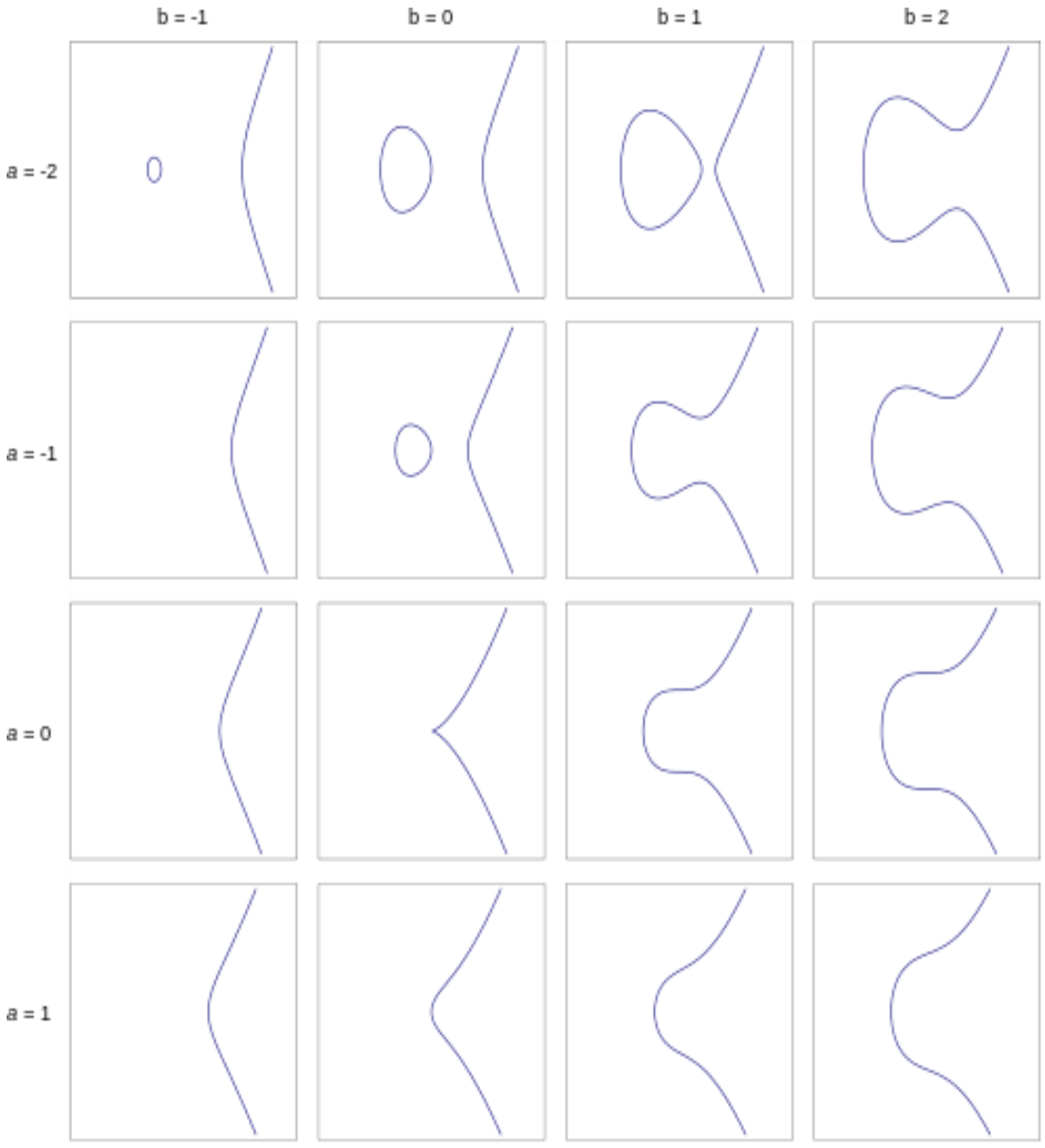

Figure 1. Elliptic curves.

The elliptic curves corresponding to whole number values of *a* between -2 and 1 and whole number values of values of *b* between -1 and 2 has been shown above (Figure 1). Only the curve for $a = b = 0$ doesn't qualify as an elliptic curve because it has a singular point.

For the sake of accuracy a couple of words need to be said about the constants a and b. for an equation of the form given above to qualify as an elliptic curve, we need that $4a^3 + 27b^2 \neq 0$. This ensures that the curve has no singular points. Informally, it means that the curve is nice and smooth everywhere and doesn't contain any sharp points or cusps. In the examples above the constants a and b were chosen to be whole numbers between -2 and 1, and -1 and 2 respectively. But in general they can also take on other values.

Given two points A and B on an elliptic curve, finding a number n such that $B = nA$ (if it exists) can take an enormous amount of computing power, especially when n is large. Elliptic curve cryptography exploits this fact: the points A and B can be used as a public key, and the number n as the private key. Anyone can encrypt a message using the publicly available public key, but only the person (or computer) in possession of the private key, the number n, can decrypt them.

4. ADVANTAGES OF ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic curve cryptography's main advantage is that smaller keys for the same level of security, especially at high levels of security can be used. ECC has some advantages over RSA cryptography – which is based on the difficulty of factorizing large numbers – as less digits are required to create a problem of equal difficulty. Therefore data can be encoded more efficiently (and thus more rapidly) than using RSA encryption [4]. Also ECC follows a two stage computation process with a good protocol for authenticated key exchange whereas RSA cryptography is slightly tricky to implement securely as its two part key is vulnerable to GCD attack if poorly implemented. Also in ECC special curves with binary pairing are really fast in hardware.

Figure 2. Hypothetical Bitcoin.

Since Bitcoin (Fig. 2) - the digital currency of today, uses elliptic curve cryptography, hence it is very much likely that more and more data is digitalised. However, it's worth noting that as yet no-one has proved that to crack elliptic curves can be difficult [3]. Hence, to solve the problem in a much shorter time there may be a novel approach. Indeed many mathematicians and computer scientists are working in this field.

5. POTENTIAL THREAT BY CRYPTOCURRENCY

One of the major problems is the potential duplication of Cryptocurrency [2] – Bitcoin. For example anyone would invent a digital currency (say Red Bull currency). He then sends it to his friend who could duplicate it and send it to 5 of his friends. This process may continue and the currency gets duplicated, thereby becoming worthless [8, 9].

Another problem is that users buy bitcoin and to conduct transactions with them there does not exist a central authority validating these transactions. Rather they all are recorded on a public ledger known as blockchain. While using online wallet investors must be sure before they trust the provider since the bitcoin could be stolen, if hackers breach its server's security measures [4].

One more big drawback is that there aren't many retailers which will accept Bitcoin as a currency though people might want to use it as it exists internationally and isn't controlled by any one government or company [10, 11].

6. CONCLUSION

Government digital spy agencies are very interested in such encryption techniques which would solve the problem of accessing large amounts of encrypted data overnight. Hence Bitcoin currency exchange would no longer be secure. This would adversely effect a lot of businesses which operate online and trade in multiple countries. It also recently transpired that the NSA has built "backdoor" entries into some elliptic curve cryptography algorithms which have allowed them to access data that the people sending it thought was secure. Mathematics is at the heart of this new digital arms race.

References

[1] Chambers Andrew, Marianne. Elliptic cryptography. Plus magazine, 20 July, 2015, 22.

[2] Lewis Hazel, Bitcoin - The currency built with mathematics. 21 December 2017. www.mathscareers.org.uk

[3] Dorothy Villa. The Nuts and Bolts of Cryptocurrency. *Planet of Finance,* 7 November 2017.

[4] Hamburg Michael. Which one is better: elliptic curve cryptography or RSA algorithm and why? *Quora* 20 November 2013, 28.

[5] George Gilder (2016). The Scandal of Money. Published in the United States by Regnery Publishing. A Division of Salem Media Group, 300 New Jersey Ave NW Washington. ISBN 978-1-62157-566-5

[6] Raymaekers, Wim. Cryptocurrency Bitcoin: Disruption, challenges and opportunities. *Journal of Payments Strategy & Systems,* Volume 9 / Number 1 / Spring, 2015, pp. 30-46(17)

[7] Kinga Kądziołka, Analysis of the investment risk in cryptocurrency Bitcoin. *Contemporary Economy* Vol. 6 Issue 3 (2015) 1-8

[8] Andrew Phillip, Jennifer S. K. Chan, Shelton Peiris. A new look at Cryptocurrencies. *Economics Letters* Volume 163, February 2018, Pages 6-9

[9] John Fry, Eng-Tuck Cheah. Negative bubbles and shocks in cryptocurrency markets. *International Review of Financial Analysis* Volume 47, October 2016, Pages 343-352

[10] Andrew Urquhart. The inefficiency of Bitcoin. *Economics Letters* Volume 148, November 2016, Pages 80-82

[11] Aurelio F. Bariviera. The inefficiency of Bitcoin revisited: A dynamic approach. *Economics Letters* Volume 161, December 2017, Pages 1-4