International Journal of
Financial Management and Economics

P-ISSN: 2617-9210
E-ISSN: 2617-9229
IJFME 2022; 5(1): 95-103
Received: 23-11-2021
Accepted: 26-12-2021

Surabhi
Research Scholar, School of Management, Gautam Buddha University, Greater Noida, Uttar Pradesh, India

Satish K Mittal
Assistant Professor, School of Management, Gautam Buddha University, Greater Noida, Uttar Pradesh, India

Corresponding Author:
Surabhi
Research Scholar, School of Management, Gautam Buddha University, Greater Noida, Uttar Pradesh, India

A comprehensive study on three pillars of cryptocurrency and blockchain technology

Surabhi and Satish K Mittal

Abstract

Bitcoin and crypto currencies are only two of the latest platitudes in financial markets. Cryptocurrencies have recently received a lot of media attention, which is one of the reasons for their present popularity. This study conceptually discusses the three pillars, cryptography, peer to peer network and proof of work, important to cryptocurrencies, due to their ever-increasing popularity as new financial instruments. The study conceptually discusses the chronology of money till cryptocurrency and their middle events. It further discusses the three necessary phenomena of cryptocurrency trading and the reason of its development as most trusted mode of payment among young population.

Keywords: Cryptocurrency, cryptography, peer to peer network, proof of work, bitcoin, double spending

1. Introduction

Nearly a decade after the first cryptocurrency was introduced, it still has the highest proportion of total market capitalization, indicating that it has the ability to replace traditional fiat currencies and change the financial services environment. Bitcoin and cryptocurrencies are only two of the latest platitudes in financial markets. Cryptocurrencies have recently received a lot of media attention, which is one of the reasons for their present popularity. But what let them go so far in such a short period of time? To better grasp the characteristics of physical monetary units and the urge to generate digital cash, we'll start with a basic trade with money.

Due to their ever-increasing popularity, cryptocurrencies, or new financial instruments, have been discussed. Some claim they are a source of illegal contributions to terrorist organisations, while others accuse them of being uncontrolled by the world's rising economies. Despite these facts, a sizable investor base continues to spend enormous sums of money into them. This might be due to the users' faith in the technology or the cryptographic principles that assure their privacy.

As a consequence, critical questions arise in everyone's minds, such as why is it spreading so rapidly? Why are so many individuals placing their faith in cryptocurrencies? What is the best bitcoin investment strategy? But, above all, we believe the most important issue is: how did it evolve? As a result, we'll start our look into the history of cryptocurrencies with the most basic form of payment: money.

We consider the debate to include themes such as money, its progression to digital money, and how it caused the problem of double spending, leading in an emphasis on the relevance of digital currency in resolving this issue. As a result, bitcoin and the technology that underpins it were introduced.

2. Literature review

Many economists argue that the faults in the barter system, the first ever medium of exchange in which ancient people exchanged commodities with one another, were the impetus for the creation of money. Money was never created as a paper note or a coin. In reality, as a guarantee of money, some monarchs had their portraits or national flags printed.

Cowry shells were the very first recorded kind of money used for commerce and trade in Asia and Africa (Kenny Li, 2018) [26]. As a guarantee, rulers used to print their faces or national symbols on paper.

The shift to coins, on the other hand, allowed monarchs to better regulate and supervise the flow and circulation of money. It allows citizens to have more confidence in money. The monarchical rule was subsequently supplanted by the government establishing its own central bank to control and distribute money in the form of paper notes and coins, ensuring that it had some value for citizens. Following this, the Hundi system was developed to easily circumvent the problem of geographical restrictions in the way of commerce or money exchange.

However, it was causing a lot of problems, so with the arrival of the internet, a new system known as digital money emerged. The only difference is that it has been converted into a digital code that the user may access at any time from any location. Debit cards, credit cards, smart cards, visa cards, and rupay cards, among other devices, all include digital codes. This new method of commerce has emerged in which the firm acts as a middleman, moving funds between buyers and sellers at any time and from any location (Bonneau, Felten, Miller, & Goldfeder, 2016) [10]. Despite all of the benefits it brought, it created a major problem of duplicate or double spending. The issue of making two payments with the same money or cash in order to deceive the recipient of those monies is known as double-spending.

The problem of duplicate spending might be eliminated with the widespread adoption of block chain technology. At this point, bitcoin began to emerge. This is due to the fact that the currencies associated with this decentralised blockchain technology go through a consensus process in order to ensure that every transaction is secure.

Evolution of cryptocurrency supported by blockchain technology started with the first digital currency or rather say, cryptocurrency known as E-cash followed by Mondex and Visa-cash. These currencies employed Cryptographic technologies to send payments both physical and digital. Blind signatures were also used by cryptographic systems to protect their users' confidentiality. There was relatively little usage and popularity, and it was largely focused on the user-merchant transaction. Because of this, e-cash failed and shops began to accept credit cards. Other currencies also met with the same fate until Bitcoin was introduced in 2009.

2.1 Cryptocurrency

Cryptocurrency, as discussed in the previous section, was introduced with the name of Bitcoin in 2009 by a person or a group of persons with pseudonym of Satoshi Nakamoto. It has become immensely popular in a very short span and has formed a new market for investors for gaining enormous returns. Since it is decentralised in nature it has always been a difficult for the governments and regulators to curb these. But it has the resemblance with money and other non-documentary securities on the basis of its matter and functions (Bolotaeva, *et al*., 2019) [9]. So, it is impossible to regulate cryptocurrency without understanding its economic nature.

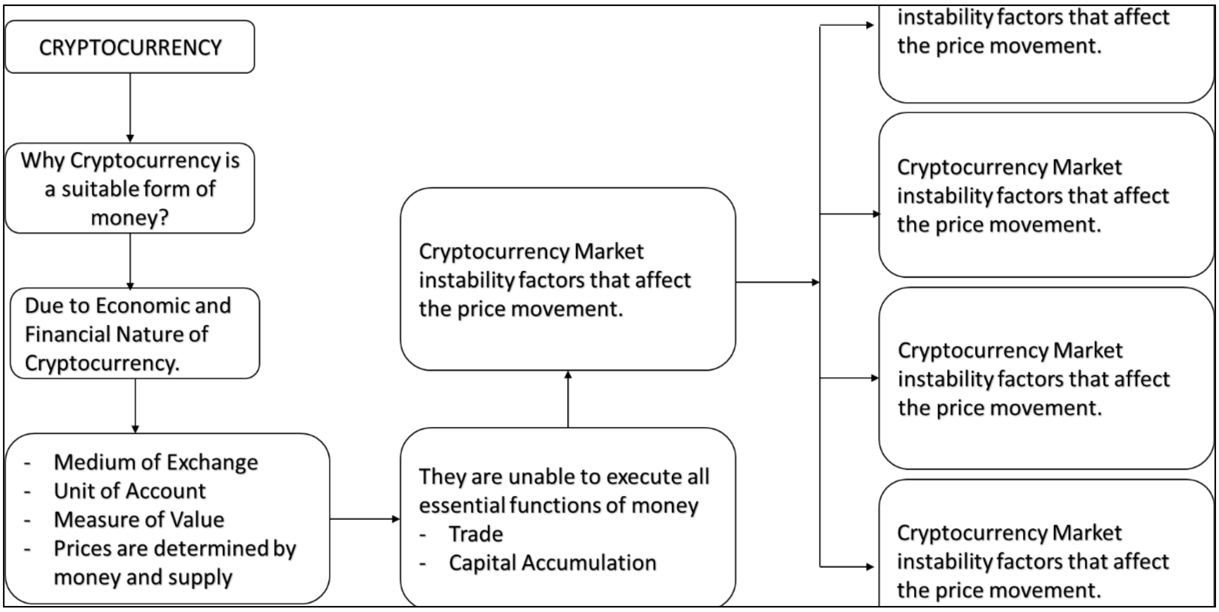

CRYPTOCURRENCY
Why Cryptocurrency is a suitable form of money?
Due to Economic and Financial Nature of Cryptocurrency.
- Medium of Exchange
- Unit of Account
- Measure of Value
- Prices are determined by money and supply
They are unable to execute all essential functions of money
- Trade
- Capital Accumulation
Cryptocurrency Market instability factors that affect the price movement.
instability factors that affect the price movement.
Cryptocurrency Market instability factors that affect the price movement.
Cryptocurrency Market instability factors that affect the price movement.
Cryptocurrency Market instability factors that affect the price movement.

Fig 1: Nature of Cryptocurrency Market

Economic nature of bitcoin and other cryptocurrencies is explained by Leonard & Treiblmaier, (2019) [28] in their significant study that it is important to note that Bitcoin serves as a medium of trade, a unit of account, and a measure of value, all of which are key functions of money. The author also finds that the volatility of Bitcoin's value, on the other hand, may function as a barrier to its usage as a means of exchange, particularly in terms of returns. As a result, if exchange rates were to become more stable, it would do even better.

If coins were made of precious metals in ancient times, and people believed their inherent value, most nations now utilise fiat money, which is backed by government assurances. In the case of cryptocurrencies, on the other hand, where the value is determined by algorithms and validated by electronic data transmission, all transaction participants are anonymous, and no authority provides a guarantee. Furthermore, in the case of cryptocurrencies, security is primarily of an IT nature, given to the cryptocurrency market’s instability and exposure to a variety of influences (Badea & Mungiu-Pupăzan, 2021) [3].

Cryptocurrencies have established themselves as vital financial technology platforms. They rely on a secure distributed ledger data structure, with mining as a major element. Mining adds past transaction records to the Blockchain distributed ledger, allowing users to reach protected, strong consensus for each transaction (Mukhopadhyay *et al*., 2016) [37]. The motivations for the rise of cryptocurrencies are not only the flaws in the conventional currency system, which has been unable to withstand multiple crises, but also the advancement of the Internet, for which cryptocurrencies potentially show to be a more suitable form of money (Srokosz & Kopciaski, 2015) [35].

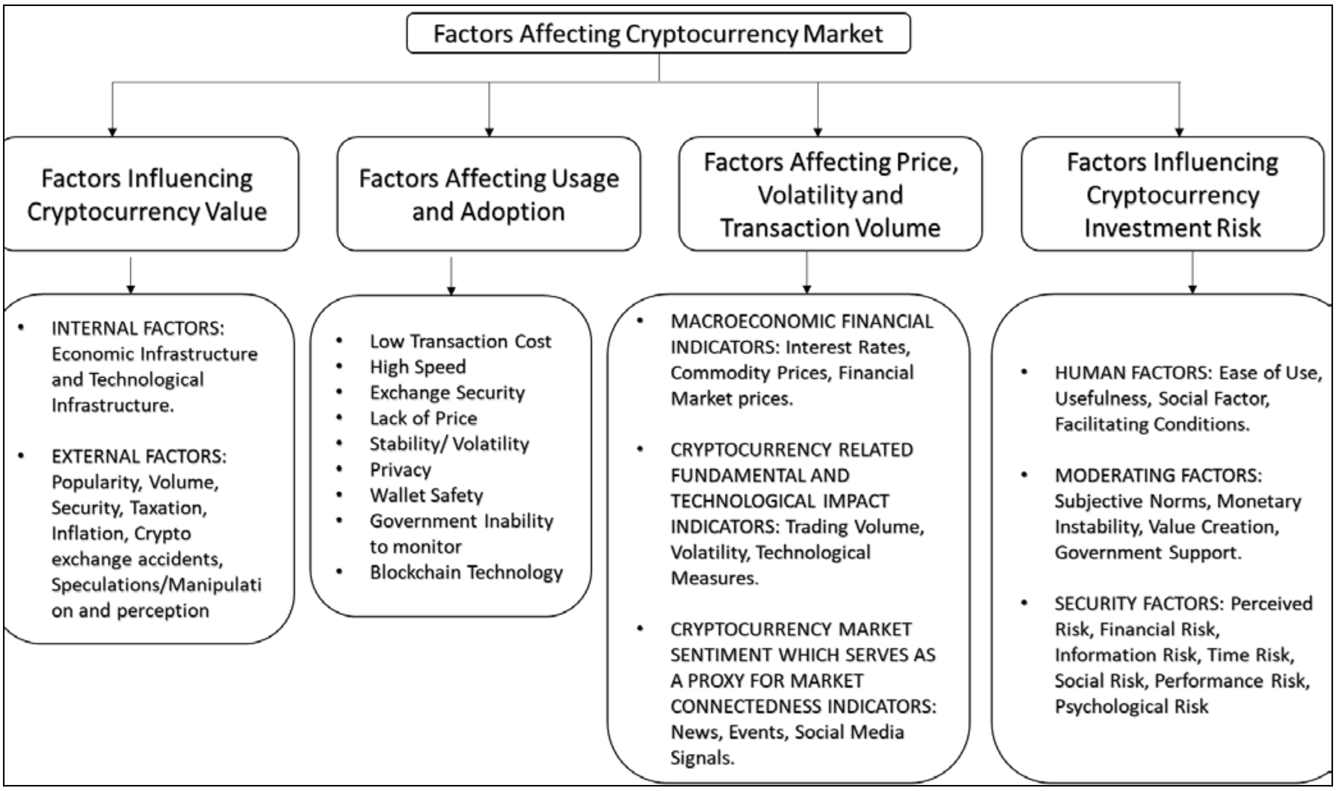

Factors Affecting Cryptocurrency Market
Factors Influencing Cryptocurrency Value
Factors Affecting Usage and Adoption
Factors Affecting Price, Volatility and Transaction Volume
Factors Influencing Cryptocurrency Investment Risk
INTERNAL FACTORS: Economic Infrastructure and Technological Infrastructure.
EXTERNAL FACTORS: Popularity, Volume, Security, Taxation, Inflation, Crypto exchange accidents, Speculations/Manipulati on and perception
Low Transaction Cost
High Speed
Exchange Security
Lack of Price
Stability/ Volatility
Privacy
Wallet Safety
Government Inability to monitor
Blockchain Technology
MACROECONOMIC FINANCIAL INDICATORS: Interest Rates, Commodity Prices, Financial Market prices.
CRYPTOCURRENCY RELATED FUNDAMENTAL AND TECHNOLOGICAL IMPACT INDICATORS: Trading Volume, Volatility, Technological Measures.
CRYPTOCURRENCY MARKET SENTIMENT WHICH SERVES AS A PROXY FOR MARKET CONNECTEDNESS INDICATORS: News, Events, Social Media Signals.
HUMAN FACTORS: Ease of Use, Usefulness, Social Factor, Facilitating Conditions.
MODERATING FACTORS: Subjective Norms, Monetary Instability, Value Creation, Government Support.
SECURITY FACTORS: Perceived Risk, Financial Risk, Information Risk, Time Risk, Social Risk, Performance Risk, Psychological Risk

Fig 2: Representation of Various Factors Affecting Cryptocurrency Market

2.2 Why Investors are considering it?

Investors are considering cryptocurrencies as an investment option other than already existing traditional forms of investments. Researchers across the world have been putting continuous efforts to understand investor’s behaviour towards these emerging currencies. Shaydullina (2018) [33] recommended regulation of cryptocurrencies based on their economic nature of being universal financial commodity, instrument and asset. Bartusiak (2018) [5] reveals, that nature of bitcoin and other cryptocurrencies is the phenomenon that possesses the basic legal properties of money. These characteristics include that cryptocurrency are decentralised and anonymous digital currency. It is a virtual asset that serves as a mode of payment and is a non-traditional money. However, Fang, *et al*. (2022) [19], in through their study suggests that cryptocurrencies and traditional currencies have many commonalities but their behaviour as an asset needs to be understood. Despite incredible price growth in recent years, cryptocurrencies have been alleged of pricing bubbles. This is due to the three reasons namely regulatory oversight, the potential for illicit use due to anonymity within a young, underdeveloped exchange system, and infrastructure breaches influenced by the rise of cyber criminality. Each has an impact on people's perceptions of cryptocurrencies as a viable financial asset class (Corbet. *Et al*., 2019) [16].

2.3 Behaviour of Cryptocurrency as an Asset

Since its inception, Cryptocurrency has been viewed as a new asset class by many marketers, researchers, and investors. This market has attracted the attentions of regulators and academics all around the world. Corbet *et al*., (2018) [15] explored the dynamic relationship between different cryptocurrencies and various financial assets and their result showed that in comparison to other assets cryptocurrencies offer diversified benefits to the investors. As a result, the research suggests that cryptocurrencies have a place in an investor's portfolio; they are highly interconnected and distinct from traditional assets, but the cryptocurrency market has its own set of hazards that are difficult to mitigate. Bitcoin and other cryptocurrencies, just like the stock market and other commodities, faced a setback during the early stages of the COVID-19 epidemic. Bitcoin's price, on the other hand, surged after October 2020. It has risen to $60,000 in March 2021. Guo & Li (2017) [13] analysed the risk in cryptocurrencies as a new investment alternative and concluded that the cryptocurrency's wealth distribution, its market consequences, and other risk factors that lead to altcoin death. In comparison to other financial markets, this figure might imply that the cryptocurrency market has experienced a favourable bounce from COVID-19 (Jalal, *et al*., 2021) [25].

3. Research methodology

To create the research's analysis, we use a case study technique to learn more about the evolution of cryptocurrencies from its inception. This qualitative case study methodology will aid academics, scholars, and investors in understanding why and how cryptocurrencies have evolved. There are numerous unknown facts that have yet to be answered or are answered in a foggy manner.

The research gives readers a better understanding of the evolution of money and cryptocurrencies. The timeline of money to cryptocurrency is studied in the paper. It will cover the three foundations of cryptocurrencies and blockchain technology, which are cryptography, proof of work, and peer-to-peer networks. The timeline of proof of work, peer to peer networks, and cryptography are also included in this research.

4. Data analysis and interpretation

A cryptocurrency, such as, Bitcoin is a type of virtual or digital money that uses encryption to prevent counterfeiting and double-spending. It resolves the problems associated with traditional currencies by providing money holders with power and accountability. It's a peer-to-peer electronic currency system. It allows online payments to be made directly from one party to another without the use of a bank.

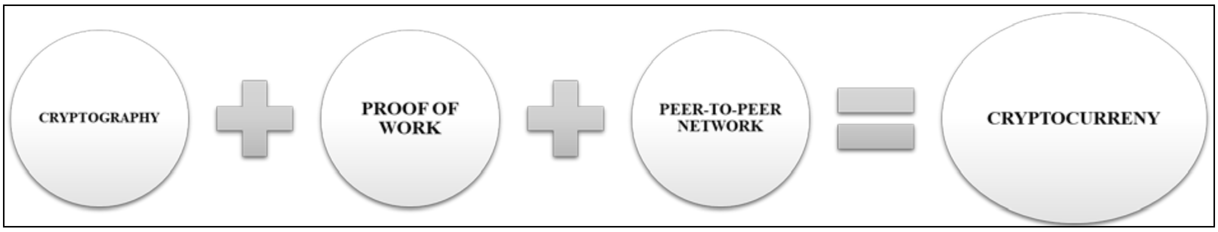


Fig 3: Three Pillars of Cryptocurrency

During the global financial crisis of 2008, Satoshi Nakamoto, a pseudonym for a person or group of individuals, issued a white paper detailing a blockchain-based implementation of a digital currency dubbed bitcoin, which was the first cryptocurrency. Bitcoin is a type of electronic payment that allows users to authenticate digital assets without depending on third parties for the first time. Combining public key cryptography, peer-to-peer networking, and a proof-of-work method achieves this.

More than a decade later, thousands of cryptocurrencies and a slew of other blockchain-based apps are widely available (Härdle, Harvey, & Reule, 2020) [23]. Investors may control their money without relying on corporations, banks, or the government because of its decentralised nature.

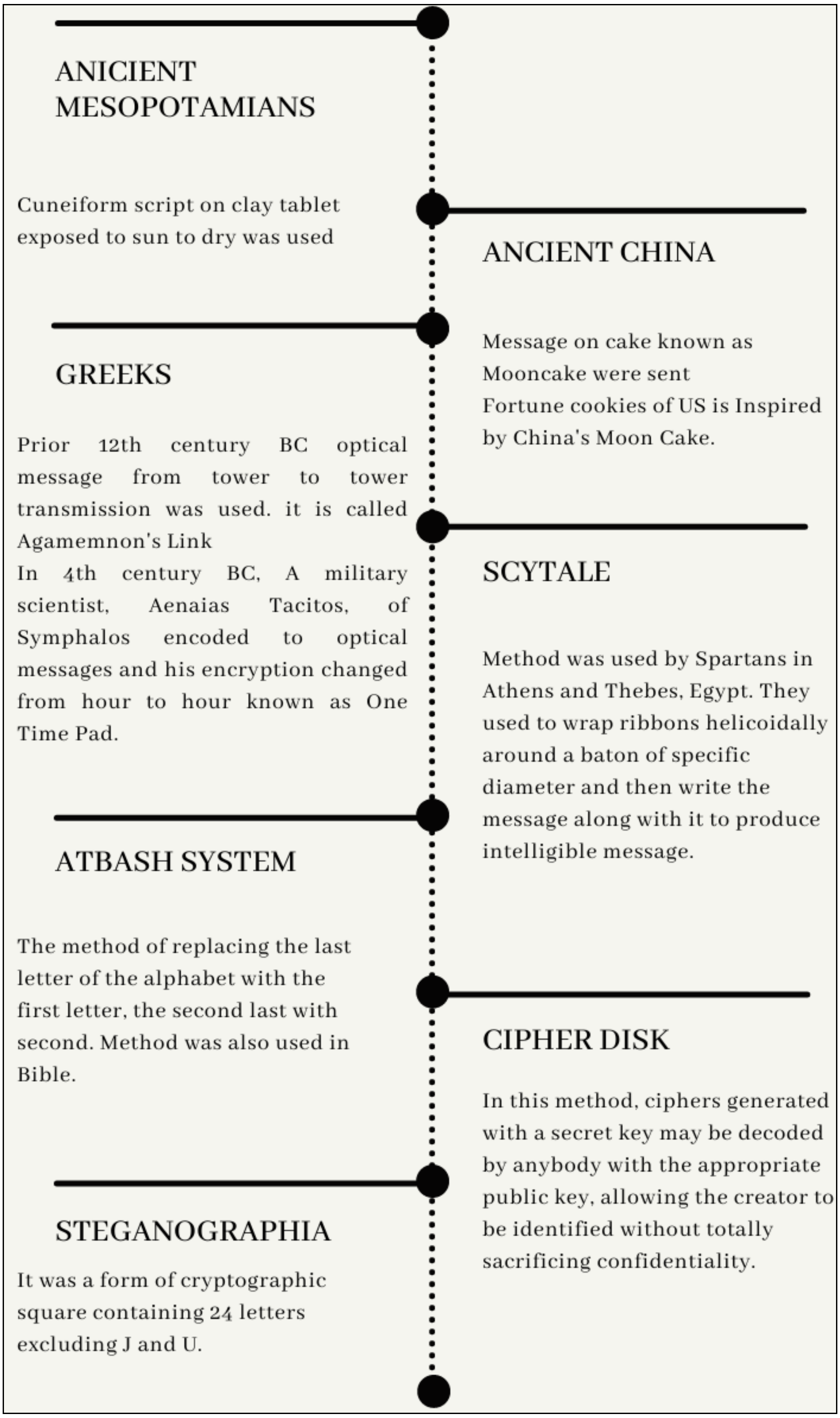
1.4.1 Cryptography

Cryptography is the safe transmission of information via the use of various methods that have been devised to ensure that only the sender and the addressee can read a message, leaving it unreadable or meaningless to a third party. Encryption is the process of converting readable data (plaintext) into incomprehensible data (ciphertext), such as files or messages, while decryption is the process of converting ciphertext back to plaintext.

The plaintext and ciphertext are linked by the use of a cypher, a cryptographic method. Each time data is encrypted, the method comprises at least one variable parameter (key). A random number generator procedure is used to create the key. A secret key is required for encryption to operate. Data conversion with a fixed key and no variable parameter (scrambling) is not included in encryption (Mann, 2002) [11].

Some consider the British computational engines conceived and built to crack the German Enigma encryption to be the first true "computers," and one might argue that cryptography is the mother of computer science (Rivest, 1990) [32]. The Caesar Cipher, developed by Julius Caesar more than two thousand years ago to convey messages to his friends, is one of the earliest encryption methods. It was one of the simplest methods of communication encryption and decryption called as Ciphertext (Rivest, 1990; Sidhpurwala, 2019) [32].

The spy service in India is described in "Arthshashtra," a famous treatise on statecraft penned by Kautalya, and discusses assigning spies' duties in "secret writing" (Sidhpurwala, 2019) [24]. For thousands of years, humans have communicated with codes and cyphers, employing basic encryption methods to safeguard trade secrets, military commands, and personal information from neighbours.



ANICIENT MESOPOTAMIANS

Cuneiform script on clay tablet exposed to sun to dry was used

ANCIENT CHINA

Message on cake known as Mooncake were sent
Fortune cookies of US is Inspired by China's Moon Cake.

GREEKS

Prior 12th century BC optical message from tower to tower transmission was used. it is called Agamemnon's Link
In 4th century BC, A military scientist, Aenaias Tacitos, of Symphalos encoded to optical messages and his encryption changed from hour to hour known as One Time Pad.

SCYTALE

Method was used by Spartans in Athens and Thebes, Egypt. They used to wrap ribbons helicoidally around a baton of specific diameter and then write the message along with it to produce intelligible message.

ATBASH SYSTEM

The method of replacing the last letter of the alphabet with the first letter, the second last with second. Method was also used in Bible.

CIPHER DISK

In this method, ciphers generated with a secret key may be decoded by anybody with the appropriate public key, allowing the creator to be identified without totally sacrificing confidentiality.

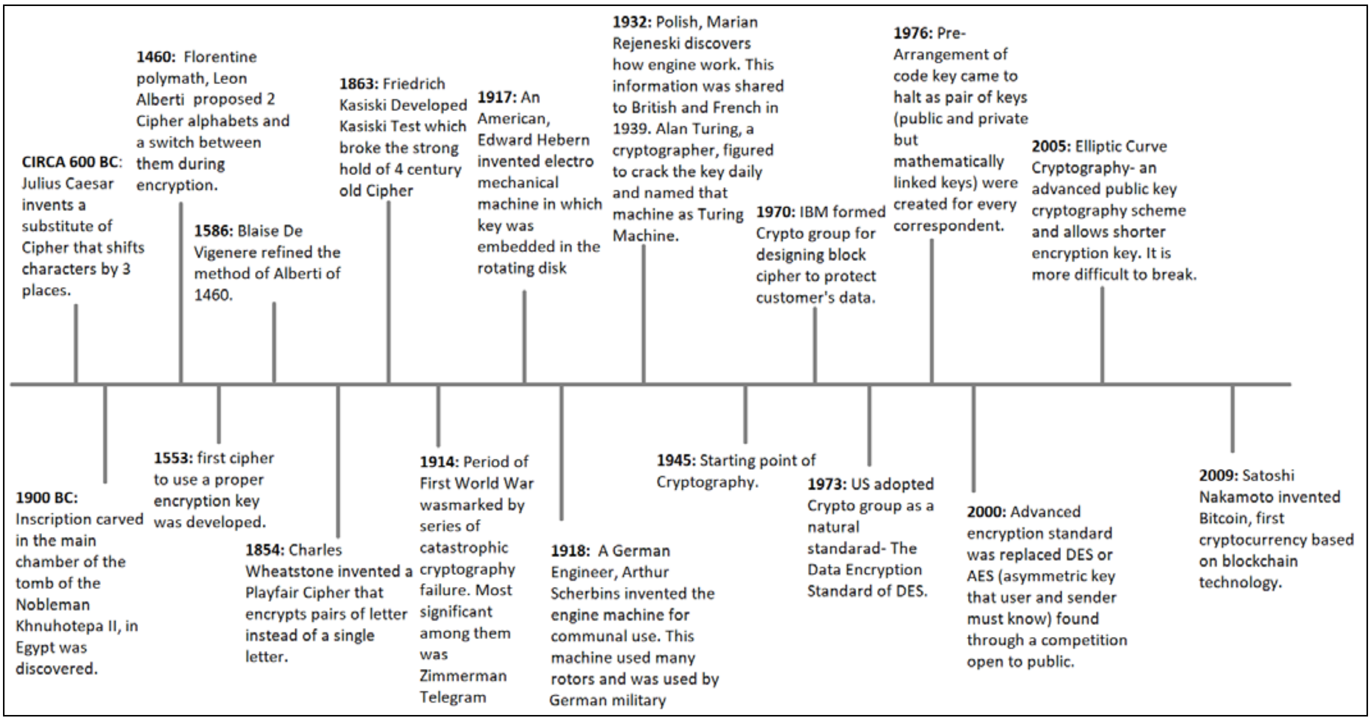
STEGANOGRAPHIA

It was a form of cryptographic square containing 24 letters excluding J and U.

Source: Author compiled from various sources

Fig 4: Ancient cryptographic communication

Any technique designed to function with a communication system in the presence of adversaries for the aim of thwarting the opponents' objectives is referred to as a cryptosystem. Cryptography is the art of building cryptosystems, whereas cryptanalysis is the art of cracking cryptosystems, and cryptology is the combination of the two (Rivest, 1990) [32].


1900 BC: Inscription carved in the main chamber of the tomb of the Nobleman Khnuhotepa II, in Egypt was discovered.
CIRCA 600 BC: Julius Caesar invents a substitute of Cipher that shifts characters by 3 places.
1460: Florentine polymath, Leon Alberti proposed 2 Cipher alphabets and a switch between them during encryption.
1553: first cipher to use a proper encryption key was developed.
1586: Blaise De Vigenere refined the method of Alberti of 1460.
1854: Charles Wheatstone invented a Playfair Cipher that encrypts pairs of letter instead of a single letter.
1863: Friedrich Kasiski Developed Kasiski Test which broke the strong hold of 4 century old Cipher
1914: Period of First World War wasmarked by series of catastrophic cryptography failure. Most significant among them was Zimmerman Telegram
1917: An American, Edward Hebern invented electro mechanical machine in which key was embedded in the rotating disk
1918: A German Engineer, Arthur Scherbins invented the engine machine for communal use. This machine used many rotors and was used by German military
1932: Polish, Marian Rejeneski discovers how engine work. This information was shared to British and French in 1939. Alan Turing, a cryptographer, figured to crack the key daily and named that machine as Turing Machine.
1945: Starting point of Cryptography.
1970: IBM formed Crypto group for designing block cipher to protect customer's data.
1973: US adopted Crypto group as a natural standarad- The Data Encryption Standard of DES.
1976: Pre-Arrangement of code key came to halt as pair of keys (public and private but mathematically linked keys) were created for every correspondent.
2000: Advanced encryption standard was replaced DES or AES (asymmetric key that user and sender must know) found through a competition open to public.
2005: Elliptic Curve Cryptography- an advanced public key cryptography scheme and allows shorter encryption key. It is more difficult to break.
2009: Satoshi Nakamoto invented Bitcoin, first cryptocurrency based on blockchain technology.

Source: Author compiled from various sources

Fig 5: Evolution of cryptography

Both the encoder and the decoder required to have a pair of exact keys until the 1970s (symmetric-key encryption). The system has two major flaws. Before the message could be sent, the key must first be provided (key exchange). Second, the number of individuals in the privy is inversely related to secrecy—intuitively, not mathematically. Furthermore, the sender has no assurance that the key was delivered to the intended recipient, and the receiver has no assurance that their key was genuine (authentication problem). This is due to the risk of a third party intercepting the key exchange and gaining access to the messages as they flow or impersonating either the sender or recipient (man-in-the-middle) (Acharya, 2017) [1]. During this time, IBM founded the Crypto group, which was responsible for developing encryption algorithm to safeguard client data. These groups were approved by the United States as the National Standard called Data Encryption Standards (DES).

1.4.2 Peer to Peer Network

Peer-to-peer (P2P) applications have grown in popularity on the Internet in recent years, ranging from file-sharing (e.g., Gnutella and FastTrack) to conferencing (e.g., End System Multicast) and content delivery (e.g., BitTorrent). "P2P" is the abbreviation for "peer to peer." The "peers" in a peer-to-peer network are computer systems that are linked to each other over the Internet. Without the use of a central server, files may be exchanged directly between systems on the network (Wang & Vassileva, 2003) [39]. It is a file-sharing system that allows users to access multimedia content such as movies, music, e-books, and games. In other words, on a P2P network, each computer serves as both a file server and a client letting hardware and software of the computer to interact. The key distinction between the two systems is that in Client-Server, there is a dedicated server with particular clients, but in P2P, it is maintained by a dispersed network of users, with each node capable of acting as both a server and a client. An Internet connection and P2P software are the only prerequisites for a computer to build a peer-to-peer network.

Table 1: Forms of peer-to-peer network

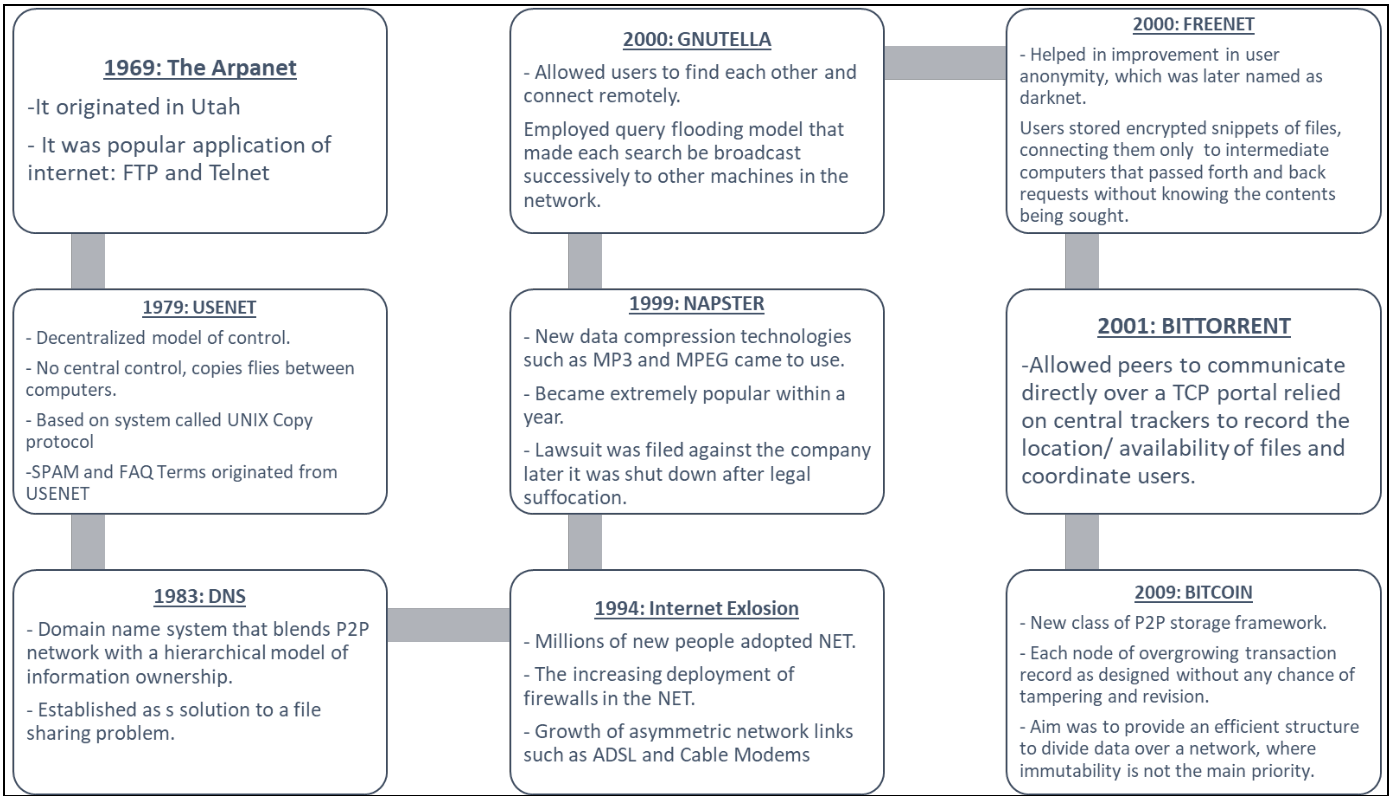
File sharing networks	Examples
Descriptive, Proof of Concept	Napster
Open Source	G Nutella
Basis of Traffic	KazaA
DHT	eDonkey,
Instant Messaging	Whatsapp, Viber, Hike, Facebook, Snapchat, Instagram
Audio Visual Conferencing	Skype, Zoom, Google meet, Anydesk, Webex
P2P Collaboration	Shared apps- File sharing, Online Games- PUBG, Clash of Clans

Source: Author compiled from various sources

While P2P networking has many legal applications, the file sharing element raises issues about intellectual property and cybersecurity. Concerns of intellectual property and copyright regulations arise whenever individuals share music, movies, software, or any other confidential data. Given the considerable and entirely legal services that P2P may fulfil, some internet service providers have sought to restrict torrents and other P2P software. P2P file sharing may also be used to spread malware, exchange or broadcast private content, and collect personally identifying information from users. Because each device aids in the routing of data over the network, they are also particularly vulnerable to denial-of-service threats (Wang & Vassileva, 2003) [39].

Apart from the disadvantages, it also has certain positives, such as P2P networking, which has a lot of advantages. In a conventional client-server network, for example, if a server goes down, the entire network falls down with it. However, in a peer-to-peer network, if one device fails, the others in the network can help take up the slack. They also ensure that network traffic is not bottlenecked at a single device by distributing traffic handling over several computers.

In case of cryptocurrency, a decentralised P2P method is used to instal the so-called P2P cryptocurrency network, which is the communication layer that transmits all data needed in the cryptocurrency system, to allow communication between various entities of a coin. The major aims of such a network are to allow members of the network to synchronise their views of the system state and to broadcast peer information so that peers can reconnect to the system after a disconnection (Delgado, *et al*., 2018) [17].



1969: The Arpanet
-It originated in Utah
- It was popular application of internet: FTP and Telnet

1979: USENET
- Decentralized model of control.
- No central control, copies flies between computers.
- Based on system called UNIX Copy protocol
-SPAM and FAQ Terms originated from USENET

1983: DNS
- Domain name system that blends P2P network with a hierarchical model of information ownership.
- Established as s solution to a file sharing problem.

1994: Internet Exlosion
- Millions of new people adopted NET.
- The increasing deployment of firewalls in the NET.
- Growth of asymmetric network links such as ADSL and Cable Modems

1999: NAPSTER
- New data compression technologies such as MP3 and MPEG came to use.
- Became extremely popular within a year.
- Lawsuit was filed against the company later it was shut down after legal suffocation.

2000: GNUTELLA
- Allowed users to find each other and connect remotely.
Employed query flooding model that made each search be broadcast successively to other machines in the network.

2000: FREENET
- Helped in improvement in user anonymity, which was later named as darknet.
Users stored encrypted snippets of files, connecting them only to intermediate computers that passed forth and back requests without knowing the contents being sought.

2001: BITTORRENT
-Allowed peers to communicate directly over a TCP portal relied on central trackers to record the location/ availability of files and coordinate users.

2009: BITCOIN
- New class of P2P storage framework.
- Each node of overgrowing transaction record as designed without any chance of tampering and revision.
- Aim was to provide an efficient structure to divide data over a network, where immutability is not the main priority.

Source: Author compiled from various sources

Fig 6: Peer to peer network timeline

1.4.3 Proof of Work

Proof-of-work (PoW) is experiencing a research resurgence so many years after its introduction by Dwork and Naor in 1992 (Laurie & Clayton, 2004; Liu & Camp, 2006) [27, 29]. PoW was designed to prevent malevolent users from obtaining more than their "fair share" of a system resource, such as bandwidth or server processing power, at first. Unsolicited mass email, commonly referred to as spam, is indeed a major issue on the Internet. If only email senders could be compelled to pay for their communications, it is proposed. PoW has become a crucial basis for cryptocurrencies like Bitcoin, as well as other blockchain technologies like Ethereum, BlockStack, and Chain Incorporated, in recent years (Gupta, Saia, & Young, 2018) [22].

Proof of work (PoW) is a type of zero-knowledge cryptographic proof in which one party (the prover) establishes to others (the verifiers) that a particular amount of computing effort has been performed. PoW refers to a system that necessitates a considerable but manageable amount of effort in order to discourage frivolous or harmful uses of computer resources, such as sending spam emails or conducting denial-of-service attacks. The essential feature of the POW functions is that they are highly expensive to solve for the email sender, but quite inexpensive to verify for the email receiver (Liu & Camp, 2006) [29]. This is the most widely used system known as Hashcash. The hashcash system is impervious by "man-in-the-middle" attacks, in which an unwitting user is tricked into computing values for the advantage of another (Laurie & Clayton, 2004) [27].

In case of cryptocurrency, Double-spending attacks and selfish mining may be avoided if all nodes in the blockchain system are closely synchronised, necessitating the use of PoW (Gervais, *et al*., 2016) [21]. The aim of the PoW feature in the Bitcoin system is to achieve consensus on the ledger history, syncing transactions and protecting users from double-spending attempts. The primary consensus algorithm in a blockchain network is Proof of Work (PoW) (Bentov, *et al*., 2016) [6]. In an environment where nodes don't trust one other, the goal of a consensus method is to bring all nodes into agreement, or trust one another. With PoW, blockchain miners compete against one another to perform network transactions and earn rewards as cryptographic scarce resources in the form of coins that can be spent inside the Bitcoin system by depleting physical scarce resources like as power and mining equipment erosion through the PoW process.

Hal Finney, a cryptographer, applied the technique of PoW to secure digital money in 2004 (Chohan, 2017) [12]. He was one of the first Bitcoin users and developers. Satoshi Nakamoto sent him 10 Bitcoins in the first transaction on the network, and he took part in it (Popper, 2014) [31]. Bitcoin was the first widely used application of Finney's PoW concept after its debut in 2009. Many other cryptocurrencies are based on proof of work, which allows for safe, decentralised consensus.

5. Discussion and Conclusion

This study has highlighted the three pillars on which cryptocurrency and blockchain technology stands. Cryptography, proof of work and peer to peer network enables the user to make electronic payment that allows users to authenticate digital assets without depending on third parties for the first time. Cryptography ensures the safe transmission of information via the use of various methods that have been devised to ensure that only the sender and the addressee can read a message, leaving it unreadable or meaningless to a third party. In cryptocurrency landscape peer to peer network is used to install cryptocurrency network, which is the communication layer that transmits all data needed in the cryptocurrency system, to allow communication between various entities of a coin. The aim of the PoW feature in the Bitcoin system is to achieve consensus on the ledger history, synchronizing transactions and protecting users from double-spending attempts.

Since everyone is talking about the cryptocurrency market and is considering it as the new investment alternative, hence it is important for them to understand the decentralised nature stands on these three phenomena. These concepts developed in ancient times and were part of human civilization since very long time period.

References

1. Acharya VV, Pedersen LH, Philippon T, Richardson, M. Measuring systemic risk. The review of financial studies. 2017;30(1):2-47.
2. Arnab Mukherjee. Origins and the history of Encryption. Digit News, 2016. https://www.digit.in/features/general/origins-and-the-history-of-encryption-30923.html
3. Badea L, Mungiu-Pupăzan MC. The economic and environmental impact of bitcoin. IEEE Access. 2021;9:48091-48104.
4. Badev AI, Chen M. Bitcoin: Technical background and data analysis, 2014.
5. Bartusiak P. «Judicial Finding» of the Legal Nature of Cryptocurrency. Ehrlich's Journal-Ерліхівський журнал. 2018;2:24-36.
6. Bentov I, Gabizon A, Mizrahi A. Cryptocurrencies without proof of work. In International conference on financial cryptography and data security. Springer, Berlin, Heidelberg, 2016, February, 142-157.
7. Berentsen A, Schar F. A short introduction to the world of cryptocurrencies, Review. 2018;100(1):1-16. SSRN.
8. Bhairav Acharya. Breaking ranks with Asia: The case for encrypting India, Observer Research Foundation, 2017. https://www.orfonline.org/expert-speak/breaking-ranks-with-asia-the-case-for-encrypting-india/#_ednref1.
9. Bolotaeva OS, Stepanova AA, Alekseeva SS. The legal nature of cryptocurrency. In IOP Conference Series: Earth and Environmental Science, June 2019;272(3):032166). IOP Publishing.
10. Bonneau J, Felten E, Miller A, Goldfeder S. Bitcoin and cryptocurrency technologies arvind narayanan. Network Security. 2016;(8):4.
11. Mann CC. A Primer on Public-key Encryption, The Atlantic, 2002. http://www.theatlantic.com/magazine/archive/2002/09/a-primer-on-public-key-encryption/302574.
12. Chohan UW. A history of bitcoin. Available at SSRN, 2017, 3047875.
13. Chuen DLK, Guo L, Wang Y. Cryptocurrency: A new investment opportunity?. The Journal of Alternative Investments. 2017;20(3):16-40.
14. Ciaian P, Rajcaniova M, Kancs DA. The economics of BitCoin price formation. Applied Economics. 2016;48(19):1799-1815.
15. Corbet S, Meegan A, Larkin C, Lucey B, Yarovaya L. Exploring the dynamic relationships between cryptocurrencies and other financial assets. Economics Letters 2018, 28-34.
16. Corbet S, Lucey B, Urquhart A, Yarovaya L. Cryptocurrencies as a financial asset: A systematic analysis. International Review of Financial Analysis. 2019;62:182-199.
17. Delgado-Segura S, Pérez-Solà C, Herrera-Joancomartí J, Navarro-Arribas G, Borrell J. Cryptocurrency networks: A new P2P paradigm. Mobile Information Systems, 2018.
18. Dourado E, Brito J. Cryptocurrency. En The New Palgrave Dictionary of Economics, 2014, 1-9.
19. Fang F, Ventre C, Basios M, Kanthan L, Martinez-Rego D, Wu F, *et al.* Cryptocurrency trading: a comprehensive survey. Financial Innovation. 2022;8(1):1-59.
20. Farell R. An analysis of the cryptocurrency industry, University of Pennsylvania, Wharton Research Scholars, 2015, 130.
21. Gervais A, Karame GO, Wüst K, Glykantzis V, Ritzdorf H, Capkun S. On the security and performance of proof of work blockchains. In Proceedings of the 2016 ACM SIGSAC conference on computer and communications security, October 2016, 3-16.
22. Gupta D, Saia J, Young M. Proof of work without all the work. In Proceedings of the 19th international conference on distributed computing and networking, January 2018, 1-10.
23. Härdle WK, Harvey CR, Reule RC. Understanding cryptocurrencies, Journal of Financial Econometrics. 2020;18(2):181-208.
24. Huzaifa Sidhpurwala. A Brief History of Cryptography 2019. https://access.redhat.com/blogs/766093/posts/1976023.
25. Jalal RNUD, Alon I, Paltrinieri A. A bibliometric review of cryptocurrencies as a financial asset. Technology Analysis & Strategic Management. 2021, 1-16.
26. Kenny Li. The History of Money & the Future of Bitcoin and the Cryptocurrency Economy, hackernoon.com, 2018.
27. Laurie B, Clayton R. Proof-of-work proves not to work. In Workshop on Economics and Information Security. 2004 May.
28. Leonard D, Treiblmaier H. Can cryptocurrencies help to pave the way to a more sustainable economy?

Questioning the economic growth paradigm. In Business transformation through Blockchain, Palgrave Macmillan, Cham, 2019, 183-205.

29. Liu D, Camp LJ. Proof of Work can Work. In WEIS June 2006.
30. Nian LP, Chuen DLK. Introduction to bitcoin. In Handbook of digital currency Academic Press. 2015, 5-30.
31. Popper N. Hal Finney, Cryptographer and Bitcoin Pioneer, Dies at 58. NYTimes. Archived from the original on. 2014, 3.
32. Rivest RL. Cryptography. In Algorithms and complexity. Elsevier. 1990, 717-755.
33. Shaydullina V. Cryptocurrency as New Economic and Legal Phenomenon. Vestnik Universiteta. 2018;(2):137-142.
34. Son Vuong T. Peer to Peer Networking: An Overview, Advanced Computer Communications, University of British Columbia, 2010. https://www.cs.ubc.ca/~cs527/Lectures2010/9a-P2P-Overview-527-10-2s.pdf.
35. Srokosz W, Kopciaski T. Legal and economic analysis of the cryptocurrencies impact on the financial system stability. Journal of Teaching and Education. 2015;4(2):619-627.
36. Thales group, (2021). A Brief History of Encryption, https://www.thalesgroup.com/en/markets/digital-identity-and-security/magazine/brief-history-encryption.
37. Mukhopadhyay U, Skjellum A, Hambolu O, Oakley J, Yu L, Brooks R. "A brief survey of Cryptocurrency systems," 2016 14th Annual Conference on Privacy, Security and Trust (PST). 2016, 745-752.
38. Valenta L, Rowan B. Blindcoin: Blinded, accountable mixes for bitcoin. In International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg. 2015 January, 112-126.
39. Wang Y, Vassileva J. Trust and reputation model in peer-to-peer networks. In Proceedings Third International Conference on Peer-to-Peer Computing (P2P2003). IEEE, 2003 September, 150-157.
40. Yermack D. Is Bitcoin a real currency? An economic appraisal. In Handbook of digital currency. Academic Press, 2015, 31-43.