INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATION & MANAGEMENT

IJRCM

CONTENTS

INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATION & MANAGEMENT   iv

A Monthly Double-Blind Peer Reviewed (Refereed/Juried) Open Access International e-Journal - Included in the International Serial Directories

http://ijrcm.org.in/

CALL FOR MANUSCRIPTS

We invite unpublished novel, original, empirical and high quality research work pertaining to recent developments & practices in the areas of Computer Science & Applications; Commerce; Business; Finance; Marketing; Human Resource Management; General Management; Banking; Economics; Tourism Administration & Management; Education; Law; Library & Information Science; Defence & Strategic Studies; Electronic Science; Corporate Governance; Industrial Relations; and emerging paradigms in allied subjects like Accounting; Accounting Information Systems; Accounting Theory & Practice; Auditing; Behavioral Accounting; Behavioral Economics; Corporate Finance; Cost Accounting; Econometrics; Economic Development; Economic History; Financial Institutions & Markets; Financial Services; Fiscal Policy; Government & Non Profit Accounting; Industrial Organization; International Economics & Trade; International Finance; Macro Economics; Micro Economics; Rural Economics; Co-operation; Demography: Development Planning; Development Studies; Applied Economics; Development Economics; Business Economics; Monetary Policy; Public Policy Economics; Real Estate; Regional Economics; Political Science; Continuing Education; Labour Welfare; Philosophy; Psychology; Sociology; Tax Accounting; Advertising & Promotion Management; Management Information Systems (MIS); Business Law; Public Responsibility & Ethics; Communication; Direct Marketing; E-Commerce; Global Business; Health Care Administration; Labour Relations & Human Resource Management; Marketing Research; Marketing Theory & Applications; Non-Profit Organizations; Office Administration/Management; Operations Research/Statistics; Organizational Behavior & Theory; Organizational Development; Production/Operations; International Relations; Human Rights & Duties; Public Administration; Population Studies; Purchasing/Materials Management; Retailing; Sales/Selling; Services; Small Business Entrepreneurship; Strategic Management Policy; Technology/Innovation; Tourism & Hospitality; Transportation Distribution; Algorithms; Artificial Intelligence; Compilers & Translation; Computer Aided Design (CAD); Computer Aided Manufacturing; Computer Graphics; Computer Organization & Architecture; Database Structures & Systems; Discrete Structures; Internet; Management Information Systems; Modeling & Simulation; Neural Systems/Neural Networks; Numerical Analysis/Scientific Computing; Object Oriented Programming; Operating Systems; Programming Languages; Robotics; Symbolic & Formal Logic; Web Design and emerging paradigms in allied subjects.

Anybody can submit the **soft copy** of unpublished novel; original; empirical and high quality **research work/manuscript** *anytime* in *M.S. Word format* after preparing the same as per our **GUIDELINES FOR SUBMISSION**; at our email address i.e. infoijrcm@gmail.com or online by clicking the link **online submission** as given on our website (*FOR ONLINE SUBMISSION, CLICK HERE*).

GUIDELINES FOR SUBMISSION OF MANUSCRIPT

1.   **COVERING LETTER FOR SUBMISSION**:

                                                                                                                          DATED: _____

THE EDITOR

IJRCM

Subject: **SUBMISSION OF MANUSCRIPT IN THE AREA OF   .**

(e.g. Finance/Mkt./HRM/General Mgt./Engineering/Economics/Computer/IT/ Education/Psychology/Law/Math/other, please specify)

DEAR SIR/MADAM

Please find my submission of manuscript entitled '_____' for possible publication in one of your journals.

I hereby affirm that the contents of this manuscript are original. Furthermore, it has neither been published elsewhere in any language fully or partly, nor is it under review for publication elsewhere.

I affirm that all the co-authors of this manuscript have seen the submitted version of the manuscript and have agreed to their inclusion of names as co-authors.

Also, if my/our manuscript is accepted, I agree to comply with the formalities as given on the website of the journal. The Journal has discretion to publish our contribution in any of its journals.

NAME OF CORRESPONDING AUTHOR	:
Designation	:
Institution/College/University with full address & Pin Code	:
Residential address with Pin Code	:
Mobile Number (s) with country ISD code	:
Is WhatsApp or Viber active on your above noted Mobile Number (Yes/No)	:
Landline Number (s) with country ISD code	:
E-mail Address	:
Alternate E-mail Address	:
Nationality	:

NOTES:

a) The whole manuscript has to be in *ONE MS WORD FILE* only, which will start from the covering letter, inside the manuscript. *pdf. version is liable to be rejected without any consideration*.

b) The sender is required to mention the following in the **SUBJECT COLUMN of the mail**:

    New Manuscript for Review in the area of (e.g. Finance/Marketing/HRM/General Mgt./Engineering/Economics/Computer/IT/ Education/Psychology/Law/Math/other, please specify)

c) There is no need to give any text in the body of mail, except the cases where the author wishes to give any **specific message** w.r.t. to the manuscript.

d) The total size of the file containing the manuscript is expected to be below **1000 KB**.

e) **Abstract alone will not be considered for review** and the author is required to submit the **complete manuscript** in the first instance.

f) *The journal gives acknowledgement w.r.t. the receipt of every email within twenty four hours* and in case of non-receipt of acknowledgment from the journal, w.r.t. the submission of manuscript, within two days of submission, the corresponding author is required to demand for the same by sending a separate mail to the journal.

g) The author (s) name or details should not appear anywhere on the body of the manuscript, except the covering letter and the cover page of the manuscript, in the manner as mentioned in the guidelines.

2. **MANUSCRIPT TITLE:** The title of the paper should be **bold typed**, **centered** and **fully capitalised**.

3. **AUTHOR NAME (S) & AFFILIATIONS:** Author (s) **name**, **designation**, **affiliation** (s), **address**, **mobile/landline number** (s), and **email/alternate email address** should be given underneath the title.

4. **ACKNOWLEDGMENTS:** Acknowledgements can be given to reviewers, guides, funding institutions, etc., if any.

5. **ABSTRACT**: Abstract should be in **fully italicized text**, ranging between **150** to **300 words**. The abstract must be informative and explain the background, aims, methods, results & conclusion in a **SINGLE PARA**. *Abbreviations must be mentioned in full*.

6. **KEYWORDS**: Abstract must be followed by a list of keywords, subject to the maximum of **five**. These should be arranged in alphabetic order separated by commas and full stop at the end. All words of the keywords, including the first one should be in small letters, except special words e.g. name of the Countries, abbreviations.

7. **JEL CODE**: Provide the appropriate Journal of Economic Literature Classification System code (s). JEL codes are available at www.aeaweb.org/econlit/jelCodes.php, however, mentioning JEL Code is not mandatory.

8. **MANUSCRIPT:** Manuscript must be in *BRITISH ENGLISH* prepared on a standard A4 size *PORTRAIT SETTING PAPER*. *It should be free from any errors i.e. grammatical, spelling or punctuation. It must be thoroughly edited at your end*.

9. **HEADINGS:** All the headings must be bold-faced, aligned left and fully capitalised. Leave a blank line before each heading.

10. **SUB-HEADINGS:** All the sub-headings must be bold-faced, aligned left and fully capitalised.

11. **MAIN TEXT**:

THE MAIN TEXT SHOULD FOLLOW THE FOLLOWING SEQUENCE:

INTRODUCTION

REVIEW OF LITERATURE

NEED/IMPORTANCE OF THE STUDY

STATEMENT OF THE PROBLEM

OBJECTIVES

HYPOTHESIS (ES)

RESEARCH METHODOLOGY

RESULTS & DISCUSSION

FINDINGS

RECOMMENDATIONS/SUGGESTIONS

CONCLUSIONS

LIMITATIONS

SCOPE FOR FURTHER RESEARCH

REFERENCES

APPENDIX/ANNEXURE

The manuscript should preferably range from *2000 to 5000 WORDS*.

12.   **FIGURES & TABLES**: These should be simple, crystal **CLEAR**, **centered**, **separately numbered** & self explained, and **titles must be above the table/figure**. **Sources of data should be mentioned below the table/figure**. *It should be ensured that the tables/figures are referred to from the main text*.

13.   **EQUATIONS/FORMULAE:** These should be consecutively numbered in parenthesis, horizontally centered with equation/formulae number placed at the right. The equation editor provided with standard versions of Microsoft Word should be utilised. If any other equation editor is utilised, author must confirm that these equations may be viewed and edited in versions of Microsoft Office that does not have the editor.

14.   **ACRONYMS**: These should not be used in the abstract. The use of acronyms is elsewhere is acceptable. Acronyms should be defined on its first use in each section: Reserve Bank of India (RBI). Acronyms should be redefined on first use in subsequent sections.

15.   **REFERENCES**: The list of all references should be alphabetically arranged. ***The author (s) should mention only the actually utilised references in the preparation of manuscript*** and they are supposed to follow Harvard Style of Referencing. **Also check to make sure that everything that you are including in the reference section is duly cited in the paper**. The author (s) are supposed to follow the references as per the following:

- All works cited in the text (including sources for tables and figures) should be listed alphabetically.

- Use (**ed.**) for one editor, and (**ed.s**) for multiple editors.

- When listing two or more works by one author, use --- (20xx), such as after Kohl (1997), use --- (2001), etc, in chronologically ascending order.

- Indicate (opening and closing) page numbers for articles in journals and for chapters in books.

- The title of books and journals should be in italics. Double quotation marks are used for titles of journal articles, book chapters, dissertations, reports, working papers, unpublished material, etc.

- For titles in a language other than English, provide an English translation in parenthesis.

- *Headers, footers, endnotes* and *footnotes* should **not be used** in the document. However, **you can mention short notes to elucidate some specific point**, which may be placed in number orders after the references.

PLEASE USE THE FOLLOWING FOR STYLE AND PUNCTUATION IN REFERENCES:

BOOKS

- Bowersox, Donald J., Closs, David J., (1996), "Logistical Management." Tata McGraw, Hill, New Delhi.

- Hunker, H.L. and A.J. Wright (1963), "Factors of Industrial Location in Ohio" Ohio State University, Nigeria.

CONTRIBUTIONS TO BOOKS

- Sharma T., Kwatra, G. (2008) Effectiveness of Social Advertising: A Study of Selected Campaigns, Corporate Social Responsibility, Edited by David Crowther & Nicholas Capaldi, Ashgate Research Companion to Corporate Social Responsibility, Chapter 15, pp 287-303.

JOURNAL AND OTHER ARTICLES

- Schemenner, R.W., Huber, J.C. and Cook, R.L. (1987), "Geographic Differences and the Location of New Manufacturing Facilities," Journal of Urban Economics, Vol. 21, No. 1, pp. 83-104.

CONFERENCE PAPERS

- Garg, Sambhav (2011): "Business Ethics" Paper presented at the Annual International Conference for the All India Management Association, New Delhi, India, 19–23

UNPUBLISHED DISSERTATIONS

- Kumar S. (2011): "Customer Value: A Comparative Study of Rural and Urban Customers," Thesis, Kurukshetra University, Kurukshetra.

ONLINE RESOURCES

- Always indicate the date that the source was accessed, as online resources are frequently updated or removed.

WEBSITES

- Garg, Bhavet (2011): Towards a New Gas Policy, Political Weekly, Viewed on January 01, 2012 http://epw.in/user/viewabstract.jsp

VIRTUAL CURRENCY – EMERGENCE OF BITCOIN

K. SHREE JYOTHI
LECTURER
DEPARTMENT OF COMMERCE
ST FRANCIS COLLEGE FOR WOMEN
BEGUMPET

Y. KALYANI
LECTURER
DEPARTMENT OF COMMERCE
ST FRANCIS COLLEGE FOR WOMEN
BEGUMPET

S. SANGEETA
ASST. PROFESSOR
DEPARTMENT OF COMMERCE
ST FRANCIS COLLEGE FOR WOMEN
BEGUMPET

ABSTRACT

Ecommerce relies on financial institutions to serve as third party to process electronic payments. The traditional model is characterized by the disputable reversible transactions. In developing countries this feature has become a stumbling block for the progress of ecommerce. This has led to the invention of virtual money. In 2008, Satoshi Nakamoto introduced a new virtual currency model called Bitcoin. The goal of this payment system is to eliminate the financial intermediaries with trust in "proof of work"(PoW). This relatively new crypto currency does have many legitimate and quickly growing uses, and best known for its popularity with criminal and shadowy internet figures. Recently, FBI became the largest owner of this Bitcoin, when it closed down the internet market place Silk Road transactions. This paper explores the concept and usage of this decentralized cryptographic currency. Growing technological advancement has triggered the popularity of virtual money and that of bit coin, though the idea of cryptographic electronic currencies came up more than two decades ago. It also looks into the SWOT analysis of the "V coin" and the future of the coin in the long run. The paper also focuses on the strength of the bit coin in comparison to the other virtual currencies that have disappeared over the time.

KEYWORDS

Bitcoin, Virtual currency, Ecommerce, P2P, Cryptography, PoW, payment systems.

INTRODUCTION

Man is the most creative species on the earth. Man's interest in exchange of goods and services for value has bought in the concept of money. Present day societies cannot function without this money. Currencies of all countries have faced the storms this decade and a search for a currency that does not experience huge fluctuations, inflation has seriously begun now, and man has matured enough to think of something that is not physical like money. The concept of money has evolved over the years. The technological innovations now have somewhat necessitated the evolution of a new concept that is accepted like the money in the digitalized "virtual world".

"Virtual Money" has been in usage since 15 years. It is now the legislators and regulators are sitting up to watch this phenomena take the financial world by surprise. In the year 2009 a crypto currency or a digitalized decentralized currency Bitcoin was introduced by Satoshi Nakomoto, a pseudonym programmer. The coin went on to become the best traded virtual currency in these five years. There are at present around 80 virtual currencies with fancy names like Feathercoin, Bbqcoin, Fireflycoin, and Zeuscoin. However unlike other cryptocurrencies, Bitcoin is supported by vibrant economy of developers, users, and exchanges, businesses that allegedly reached a $2.5B market cap at the end of April 2013. This "V coin" has acquired importance because the currency supports new forms of e-commerce, online business formats and challenges established the financial system.

This paper explores the trend of these virtual currencies with special reference to Bitcoin. It is important to take into account that these currencies both resemble money and necessarily come with their own dedicated retail payment systems; these two aspects are covered by the term "virtual currency scheme" Bit coin's emergence as the most popular virtual currency is of special interest to central banks as these have threatened the existence of financial intermediaries like banks. They have somehow grown without the regulatory noose of the central Banks around the world. This paper tries to trace the rise of Bitcoin, its resilience to financial downturns or crisis. The study is mainly an exploratory one and hence tries to arrive at a possible hypothesis that can be studied further. There has been a spate of debates and discussions across the western world about this Bitcoin. In India the Bitcoin seems to be in the nascent stage only and the RBI has not acknowledged its existence as yet.

The study is limited to the exploring of present literature on virtual currencies. This is an emerging idea and there is not much authentic literature on the subject. The study depended on internet publications and some of the publications made by banks in US, European Central bank and National Australian bank. This is the major limitation of the study. The concept of crypto currencies depends mainly on computer software systems, which are difficult for layman's understanding posing a limitation. The mining of these coins requires a reasonable level of computer knowledge. With India being one of the major countries bestowed with best of computer software personnel, we may assume a potential market in India for this Bitcoin, thus the study explores the SWOT of this currency to become the future of all financial transactions.

VIRTUAL CURRENCY

Dictionary definition of 'Currency" is a system of money in general use in a particular country: the fact or quality of being generally accepted or in use. Virtual is something that is not visible, physical. These currencies are virtual because they are not physical and are not backed by any physical commodity of value like gold or similar goods. The history of currency shows that it has evolved over the time and that it need not necessarily be physical. However, there are certain characteristics that are mandatory for it to be currency.
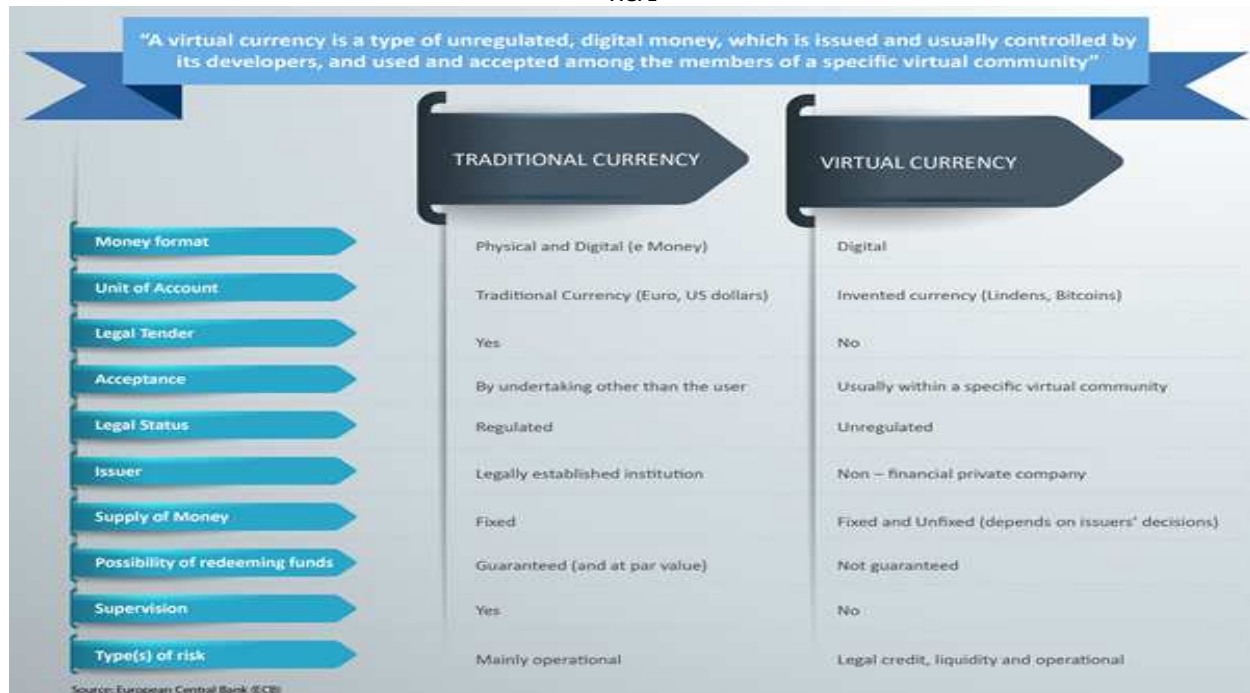
- Medium of exchange
- Unit of account

- Store of value
- Restricted supply

The test that any medium of exchange becoming a currency has to stand up to is the trust or acceptability it enjoys, the value it creates for itself, user, and creator. Thus there is a significant level of perception of the users involved in the concept of currency.

Apart from the difference that the traditional currency is physical and the virtual currency is digital, the difference between a traditional currency and virtual currency is that the traditional currency has central agencies as its creators while virtual currencies are not created by any central agency. The second difference is that the traditional currency is regulated by the central agency while the virtual currency is not under any regulatory authority.

FIG. 1

"A virtual currency is a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community"

	TRADITIONAL CURRENCY	VIRTUAL CURRENCY
Money format	Physical and Digital (e Money)	Digital
Unit of Account	Traditional Currency (Euro, US dollars)	Invented currency (Lindens, Bitcoins)
Legal Tender	Yes	No
Acceptance	By undertaking other than the user	Usually within a specific virtual community
Legal Status	Regulated	Unregulated
Issuer	Legally established institution	Non – financial private company
Supply of Money	Fixed	Fixed and Unfixed (depends on issuers' decisions)
Possibility of redeeming funds	Guaranteed (and at par value)	Not guaranteed
Supervision	Yes	No
Type(s) of risk	Mainly operational	Legal credit, liquidity and operational

Source: European Central Bank (ECB)

Virtual money is anything other than the real money used for the exchange of goods. Usage of cards, gift vouchers, passes etc also has the same unregulated anonymity of cash transactions. Virtual money saw it's beginning some fifteen years ago. The beginning has been in the games where the coins like the Linden dollars or any other points earned on your credit card, or points earned on your Face book account, which can be later, exchanged for any goods offered by the particular company, community on the computer. The European Central Bank in its report on virtual currency schemes in October 2012 classified the present currencies under three categories. These are the closed virtual currency scheme, unidirectional flow of virtual currency scheme and virtual currencies with bi-directional flow.

The increase in the various online businesses combined with the increase in the technological progress facilitated or gave impetus to this phenomenal growth in the virtual economies and currencies. This preposition has attracted the watchful eyes of regulatory central banking authorities world over.

The challenge that these virtual currencies face is the supply or restricting the creation and avoiding the duplication of its use. This is solved to some extent through complex software programming that ensures the limited supply as well as authentication of the transaction and not allowing duplication. Bit coin's supremacy lies in its features which stand to these two challenges.

RELATED WORK

Satoshi Nakamoto (2009) proposed a system for electronic transactions without relying on trust. His model started with usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double spending.

In three frequently cited articles, **Kocherlakota and Wallace** (1998) and **Kocherlakota** (1998; 2002b) consider the similarities and substitutability of money and memory. William J. Luther, Josiah Olson, **Kenyon College**, stated that the Theories of memory have practical applications. Bitcoin is an imperfect form of memory and traditional monies are costly to store and/or verify, it is possible for the two types of exchange medias to coexist. **Philipp Güring, Ian Grigg**(2011) concluded that the requirement of diversification is broken by Bitcoin's very mechanism to make diversification work fairly. **Meni Rosenfeld** November 17, 2011, introduced Bitcoin mining and explained why the high variance in the rewards for this activity creates the need for mining pools. **Meni Rosenfeld** December 11, 2012, derived the probability for a successful double-spend, and tabulated it in various ways. **Ilja Gerhardt, Timo Hankey** (2012), introduced a payment protocol for customer merchant relations. A public key identifies merchants, which is their pseudonym. The protocol is suitable for bitcoin as the underlying payment system. **Denis Jaromil Roio**, 6 April 2013, claimed Bitcoin is breaking the Taboo on Money. He also said that it is a system that permeates most if not all-societal interactions, at least in the Western world, so it is assumed it to be neutral and, in any case, its existence cannot be questioned.

WORKING OF BITCOIN

Bitcoin is a giant digital ledger of individual coins (bitcoins – small letter b) where each entry is eventually tamper proof. Individual wallets carry a balance by referencing entries in the ledger, which point to them being the destination of the last transaction for a particular coin. Each wallet is a digital address, which can be referenced in such as transaction.

A physical entry such as an individual or a business or any commercial entity can have multiple wallets. A wallet is not a summary of holdings. It should be viewed as the entities own ledger balance of currently valid references to coins, similar to a commercial commodities account. However, unlike any such account, which cannot be easily "stolen", a wallet can be stolen by physically copying its underlying secret key (it's private key). Hence,the model of an electronic wallet.

One can use bitcoins from this point on as an international currency similar to the US Dollar. The stakeholders in the bitcoin network are the users who hold wallets, the bitcoin network, which maintains a global record of each bitcoin and merchants who accept bitcoin as a payment currency similar to other local currencies. Some of the types of merchants are normal businesses like retailers. There are even exchange style retailers who buy and sell other currencies in exchange for bitcoin either way.

INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATION & MANAGEMENT   54

A Monthly Double-Blind Peer Reviewed (Refereed/Juried) Open Access International e-Journal - Included in the International Serial Directories

http://ijrcm.org.in/

Bitcoin is based on the economics of value, as bitcoins inherently carry no value. It is the value advertised by a merchant and accepted by a buyer, which determines a bitcoin's underlying value. In essence then, Bitcoin should be viewed as one of the ways in which a free market is evolving. The advantages it offers over the currently prevalent one of debt-backed currencies are

1) Elimination of "trust" as a basis for trade. Bitcoin is designed to always validate transactions coin by coin and works on the premise of not trusting anyone. This leads to elimination of currency fraud such as currency counterfeiting as a risk. Risks of fraud due to inadequate or fraudulent service still remain and should be covered by consumer protection legislation from the seller's country.
2) Elimination of unequal players in the market such as central banks who vary the value of a currency by regulating its supply/issuing debt.
3) A ceiling on the unregulated expansion of money supply and subsequent non-market backed inflation. The total number of possible bitcoins possible mathematically is limited to 21 Million as a hard limit.
4) Means for users to participate in a global market with an unregulated currency. This prevents any third party from interfering within any transaction

MECHANICAL ASPECTS OF BITCOIN

There are about 10 million bitcoins in existence today. When the Bitcoin network started, the value was obviously 0. So there is a process by which bitcoins are introduced in the economic system. One should view this analogously to the old system of precious metals as currency where a gold miner was effectively creating currency. The difficulty of finding and refining gold as an acceptable medium of commercial exchange established a value to this mining process.

An intentionally named process of mining creates Bitcoins. Bitcoins are special sequences of bits within blocks, which have to satisfy many conditions. They have to be generated in blocks in pre-determined intervals only. This is again intentional as some of these conditions are crucial to establishing integrity within the Bitcoin (or BTC) network.

Every block introduces 50 new coins in the system. This quantity (50) halves every 210,000 blocks. So, getting the limit of coins it is possible to generate is quite easy: it's the sum of a geometric series.

$$\sum_{n=0}^{\infty} \frac{210000 \times 50}{2^n} = 210000 \times 50 \times \frac{1}{1 - \frac{1}{2}} = 21000000$$

(This is an upper bound; the actual quantity will probably be a bit lower due to rounding issues (BTC has a finite number of decimals, 8).

Bitcoins will cease to be generated after a point in time by design.

GRAPH 1

Total Bitcoins over time
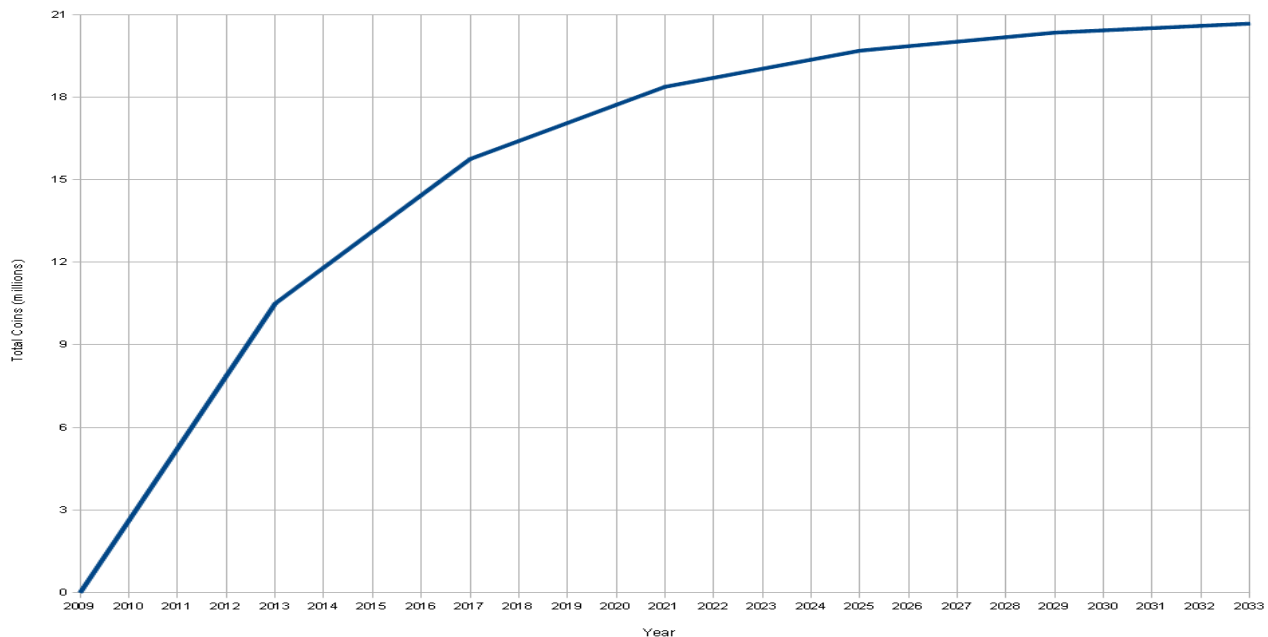
The Bitcoin network consists of a ledger of each and every known bitcoin, which double up as the input needed to mine new bitcoins. Nodes, which maintain these ledgers today, spend time and energy in finding a sequence of bits (32 characters), which precisely satisfy the many conditions for a valid solution to the mathematical problem, which will ultimately generate a valid bitcoin.

BITCOIN MINING AND TRANSACTION INTEGRITY TODAY

In the Bitcoin network, all outstanding transactions involving a transfer of ownership of bitcoins (note that we do not say transfer of bitcoins) are gathered together in a block of unconfirmed transactions worldwide. These are unconfirmed, as they are not yet entered into the digitally signed block based ledgers of the computer network worldwide. Today's mining algorithm is based on

1) Gather a list of potential transactions known as a "block". This list of transactions comes from the outstanding transactions in the worldwide list. It is not necessary that all transactions be found – simply because a block of transactions may be composed out of a large enough set of local transaction, local to a set of computers maintaining their ledgers and exchanging information about them. Since this set of computers is worldwide, this list or block of transactions is not necessarily identical. If a transaction does not make it into a successful block, it will make it into the next one, as all transactions will be public and known worldwide soon. The rate of spread is effectively the speed of the Internet. Two computers at opposite ends of the network may create blocks with many common transactions and some dissimilar ones. Once of these blocks will be successfully added to the global network. The remaining transactions in the unsuccessful block will be known worldwide by then so they become candidates for subsequent blocks. Eventually they will make it into a block. Since the time taken cannot be bound as can be seen, confirming a transaction on the Bitcoin network takes time.
2) Calculate a hash for a block of potential transactions along with a random number.
3) If the hash is more than the currently set difficulty level, then you have mined that block. If not, start over from step 1. Any additions to the list of transactions from step 1 along with change in the random number from step 2 mean that there's a chance that the criterion will be met in the next go around.

This description is simplified and omits a few details to communicate the basic idea.

WHAT'S A HASH?

A **cryptographic hash** (sometimes called 'digest') is a kind of 'signature' for a text or a data file. SHA-256 generates an almost-unique 256-bit (32-byte) signature for a text. See this website (http://www.movable-type.co.uk/scripts/sha256.html) to try this out yourself.

Enter any message to check its SHA-256 hash

- Message
- Hash
- *Note SHA-256 hash of 'abc' should be: ba7816bf8f01cfea414140de5dae2223b00361a396177a9cb410ff61f20015ad*

A hash is a function that converts data into a number within a certain range. The hash has the property that knowing it's output is essentially unpredictable (within the given range). The specific hash function used for bitcoin mining is SHA256 applied twice.

CONFIRMATION TIME

By design, each block takes about 10 minutes to solve; so waiting for 6 blocks would take about an hour. The particular choice of 10 minutes is an arbitrary time interval to ensure even slow networks get to exchange transaction information. As more computers join the network, and specialized hardware is designed specifically for mining, the block solution time would get very small. To compensate, every two weeks, all the Bitcoin software recalibrates the difficulty of the math problem to target 10 minutes. For comparison, a similar digital currency called Litecoin has been able to operate with a 2.5 minute block time.*

*A paper by M. Rosenfeld, Analysis of hashrate-based double-spending, concludes that security is a function of the number of blocks, and not the time used to solve each block, but this assumes an attacker's computing power is not dependent on time, i.e., he could overpower the network for days just as easily as a few minutes.

*Also see comments by Satoshi regarding block time and system efficiency: https://bitcointalk.org/index.php?topic=130222.60

HOW DOES THE DIFFICULTY LEVEL WORK?

This unpredictable nature of the hash function (the solution space is spread across the possible combination of 256 bits such that the leading set of bits are 0) means that putting in random data (the transaction + the random number) will essentially produce a random number within a certain range. Further restricting the range of the desired output affects how likely one is to find it in a single round. This creates a way to probabilistically determine how often a solution will be found based on the number of times the algorithm can be run on the network. Specifically, when you hear the term Gigahashes or Terrahashes, this refers to the number of times step 3 can be run. As the number of hashes per second across the entire network grows, the network automatically raises the difficulty such that a solution will be found within about 10 minutes.

Example block hashes

Hash	00000000000000038e96358b0c7aaaf69d63bac03820d5b47d59c9d00019c722
Previous Block	000000000000000202b99385096abf80d615ebe4f31153b30dd0fcf34e1e10dc
Next Block(s)	000000000000000029e7ab1e48711605ee6c0fdddcd7c87e0631c01548415d0b

To see this network in action, one can navigate to http://blockchain.info and pick any block chain to see transactions in flight.

WHAT HAPPENS WHEN A BLOCK IS MINED?

When a block is mined, the miner sends the block to all other miners on the network as evidence that it has found it. This block contains a list of transactions, the found hash, the specific random number, and a reference to the previous hash. As each miner receives the newly mined block, it removes all transactions that it is currently mining that exist within the block (because they've already been confirmed in the block chain) and broadcasts the block to other miners that do the same thing. The propagation happens pretty quickly. Note: the original miner of the block gets a "miners' fee", which is a reward the any unspent coins from transactions in addition to a "coinbase" reward, which stated out at 50 bitcoins and halves after ever 20... blocks. The coinbase reward will eventually get so small that it will be miniscule compared to miner's fees.

SWOT ANALYSIS

TABLE 1

	Strengths	Weaknesses
I	1. Easy access	1) Large amount of computer power required
N	2. Great marketability	2) Scarcely available
T	3. Good security	3) Time consuming
E	4. Quick multiplicability	4) Requires expensive computing services
R	5. Demand	5) Its use is limited
N	6. Avoid duplication of use	6) Liquidity problems
A	7. Durability	7) Not redeemable like other currency
L	8. Portability	
	9. Fungibility	
	10. Divisibility	
	11. Valuable	
	12. Self regulating Currency	
	13. Avoids physical and logistical problems	
	14. Anonymity	
	15. Lack of intermediary	
	16. Immediacy of settlement	
	17. Wide acceptance	
	18. Untraceability	
	Opportunities	Threats
E	1. Increase in various online businesses	1. Restriction in supply of virtual currency
X	2. Technological progress	2. Regulations of various nations
T	3. Bitcoin exchange markets	3. Illegal activities
E	4. Overseas remittances	4. Tax considerations imposed
R	5. Financial inclusion	5. Highly Speculative in nature
N		6. Possess financial risk
A		7. Absence of distinct legal framework
L		8. Transactions are irreversible
		9. Hacking of private key leading to loss of money (Silk Road)

CONCLUSION

Bitcoin is a great innovation, which is beneficial for ebusiness. Bitcoins have value because they are useful as form of money. Bitcoin's clever use of public-key encryption and peer-to-peer networking solves the double-spending problem that had previously made decentralized digital currencies impossible. Bitcoin when analysed on the basis of SWOT turned out to be a strong virtual currency with some dangerous limitations like illegal activities and frauds. Bitcoin is more

amenable to government regulation. Bitcoin, which is designed to allow individuals to make transactions directly without financial intermediaries, has attracted significant attention recently because of the challenges of regulating the system. The rules can be changed. They have been changed. And a semi-formal Bitcoin governance process is emerging. To the extent that Bitcoin's governance structure is subject to pressure from a regulator, or that a significant fraction of miners or users are subject to regulatory pressure, the regulator will be able to put pressure on the Bitcoin economy to change its rules. Even if a regulator forces the developers to incorporate changes into the Bitcoin rules and reference software, the rest of the Bitcoin community will be able to fork the rules and carry on under the rule set of its choice. Bitcoin is not immune to regulation, but it is not like traditional currencies either. Bitcoin is the mainstream open-source currency.

REFERENCES

1. A. Back et al. Hashcash-a denial of service counter-measure. http://www.Hashcash.org/papers/hashcash.pdf, 2002.
2. A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in CRYPTO '86, vol. 263 of LNCS, 1986, pp. 186–194.
3. A. Narayanan and V. Shmatikov, "De-anonymizing social networks," in Security and Privacy, 2009 30th IEEE Symposium on. IEEE, 2009, pp. 173–187.
4. "Bitcoin fog company," http://www.bitcoinfog.com/.
5. "Blind Bitcoin," Information at https://en.bitcoin.it/wiki/Blind Bitcoin Transfers.
6. D. Ron and A. Shamir, "Quantitative Analysis of the Full Bitcoin Transaction Graph," Cryptology ePrint Archive, Report 2012/584, 2012, http://eprint.iacr.org/.
7. E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun. Evaluating User Privacy in Bitcoin. In Proceedings of Financial Cryptography, 2013.
8. European Central Bank, "Virtual currency schemes," Available at http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf, October 2012.
9. F. Reid and M. Harrigan, "An analysis of anonymity in the Bitcoin system," in Privacy, security, risk and trust (PASSAT), 2011 IEEE Third Internatiojn Conference on Social Computing (SOCIALCOM). IEEE, 2011, pp. 1318–1326.
10. http://bitcoin.org. Bitcoin - P2P Digital Currency
11. http://dx.doi.org/10.1007/s13389-013-0057-3
12. http://moneymorning.com/2013/11/22/why-virtual-currency-is-here-to-stay-bitcoin-or-no-bitcoin/
13. http://ovum.com/2013/06/10/bitcoin-hype-ignores-the-challenges-of-gaining-financial-legitimacy/
14. http://www.btcguild.com. BTC Guild.
15. http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf
16. https://bitcoinfoundation.org. Bitcoin Foundation
17. https://en.bitcoin.it/wiki/BIP 0016
18. https://www.torproject.org/
19. J. Becker, D. Breuker, T. Heide, J. Holler, H. Rauer, and R. B ohme. Can We A_ord Integrity by Proof-of-Work? Scenarios Inspired by the Bitcoin Currency. In Workshop on the Economics of Information Security, 2012.
20. J. Benaloh and M. de Mare, "One-way accumulators: a decentralized alternative to digital signatures," in EUROCRYPT '93, vol. 765 of LNCS, 1994, pp. 274–285.
21. J. L. Camenisch, "Group signature schemes and payment systems based on the discrete logarithm problem," Ph.D. dissertation, ETH Z¨urich, 1998.
22. Kocherlakota, Narayana R. 1998. "Money is memory." *Journal of Economic Theory*, 81(2): 232-51.
23. Kocherlakota, Narayana R. 2002a. "Money: what's the question and why should we care aboutthe answer?" *American Economic Review*, 92(2): 58-61.
24. Kocherlakota, Narayana R. 2002b. "The two-money theorem." *International Economic Review*, 43(2): 333-346.
25. M. Babaio_, S. Dobzinski, S. Oren, and A. Zohar. On Bitcoin and Red Balloons. In Proceedings of the 13th ACM Conference on Electronic Commerce, pages 56{73. ACM, 2012.
26. Reuben Grinberg. "Bitcoin: An Innovative Alternative Digital Currency." *Hastings Science & Technology Law Journal* 4 (2011): 160–208. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1817857
27. S. Barber, X. Boyen, E. Shi, , and E. Uzun. Bitter to Better|How to Make Bitcoin a Better Currency. In Proceedings of Financial Cryptography, 2013.
28. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system,2009," 2012. [Online]. Available: http://www.bitcoin.org/bitcoin.pdf
29. T. B. Lee, "A risky currency? Alleged $500,000 Bitcoin heist raises questions," Available at http://arstechnica.com/, June 2011.
30. "The Bitcoin Laundry," http://www.bitcoinlaundry.com/.
31. The Bitcoin wiki. *The Bitcoin wiki*. Apr. 2012. url: https://bitcoin.it

REQUEST FOR FEEDBACK

Dear Readers

At the very outset, International Journal of Research in Computer Application & Management (IJRCM) acknowledges & appreciates your efforts in showing interest in our present issue under your kind perusal.

I would like to request you tosupply your critical comments and suggestions about the material published in this issue as well as on the journal as a whole, on our E-mail**infoijrcm@gmail.com** for further improvements in the interest of research.

If youhave any queries please feel free to contact us on our E-mail **infoijrcm@gmail.com**.

I am sure that your feedback and deliberations would make future issues better – a result of our joint effort.

Looking forward an appropriate consideration.

With sincere regards

Thanking you profoundly

Academically yours

Sd/-
Co-ordinator

DISCLAIMER

The information and opinions presented in the Journal reflect the views of the authors and not of the Journal or its Editorial Board or the Publishers/Editors. Publication does not constitute endorsement by the journal. Neither the Journal nor its publishers/Editors/Editorial Board nor anyone else involved in creating, producing or delivering the journal or the materials contained therein, assumes any liability or responsibility for the accuracy, completeness, or usefulness of any information provided in the journal, nor shall they be liable for any direct, indirect, incidental, special, consequential or punitive damages arising out of the use of information/material contained in the journal. The journal, neither its publishers/Editors/ Editorial Board, nor any other party involved in the preparation of material contained in the journal represents or warrants that the information contained herein is in every respect accurate or complete, and they are not responsible for any errors or omissions or for the results obtained from the use of such material. Readers are encouraged to confirm the information contained herein with other sources. The responsibility of the contents and the opinions expressed in this journal are exclusively of the author (s) concerned.

ABOUT THE JOURNAL

In this age of Commerce, Economics, Computer, I.T. & Management and cut throat competition, a group of intellectuals felt the need to have some platform, where young and budding managers and academicians could express their views and discuss the problems among their peers. This journal was conceived with this noble intention in view. This journal has been introduced to give an opportunity for expressing refined and innovative ideas in this field. It is our humble endeavour to provide a springboard to the upcoming specialists and give a chance to know about the latest in the sphere of research and knowledge. We have taken a small step and we hope that with the active co-operation of like-minded scholars, we shall be able to serve the society with our humble efforts.

Our Other Journals