iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** IX **Month of publication:** September 2022

DOI: https://doi.org/10.22214/ijraset.2022.46538

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IX Sep 2022- Available at www.ijraset.com

A Comprehensive Study on Namecoin

Alisha Gupta[1], Rishabh Chopda[2], Bhushan Chaudhary[3], Pratibha Dwivedi[4], Sangeeta Vhatkar[5]
[1, 3, 4, 5]*Information Technology,* [2]*Computer Engineering, Thakur College Of Engineering &Technology Kandivali East, Mumbai*

Abstract: ***Financial transaction networks are among the world's biggest networks. The digital (crypto) currency network, such as Bitcoin, is a relatively new sort of financial network. Namecoin is a cryptocurrency that is based on Bitcoin and includes functionalities such as DNS. The Namecoin network has nearly 17 million edges and over 2 million nodes. The analysis of such a crypto currency network can aid in the modelling or prediction of future transaction network growth. We evaluated the Namecoin blockchain data in 7 six-month periods in order to analyse the transaction network graph over time. In comparison to Bitcoin, our data imply that user behaviour and development patterns are different [1]. "An experimental open-source technology that improves the decentralisation, security, censorship resistance, privacy, and speed of certain components of the Internet infrastructure, such as DNS and identities," according to Namecoin's definition.***
Keywords: Namecoin, Bitcoin, network, crypto currency, Internet

I. INTRODUCTION

Namecoin proponents feel that a decentralised DNS system is essential for long-term Internet privacy and censorship reduction. While most people are unlikely to require a.bit website or associated service, Namecoin might give certain people the tools they need to access to an Internet free of censorship and central control. Despite the fact that we input text-based website URLs into Internet browsers, the Internet is essentially built on numerical numbers known as IP addresses. The DNS was established to make Internet navigation easier since a large string of numbers is difficult to memorise [2]. The Domain Name System (DNS) is the Internet's address book. A DNS server is called every time you enter in a website address. The DNS server determines the IP address of the Internet destination server before retrieving the data for that web page. The top-level domain (.com) is the last portion of a website's domain (TLD). A central authority is in charge of all TLDs. The Internet Corporation for Assigned Names and Numbers, for example, manages the top-level domain.com (ICANN). When a specific complaint about a webpage develops, the TLD's central authority has final say over how the issue is resolved. Lawyers or copyright proprietors will connect with the central authority in the vast majority of real-world issues. Those concerned about censorship, on the other hand, may find the existence of any central authority with the capacity to issue directives troublesome.

TLDs that are not controlled by any individual can now exist as a result of the implementation of a decentralised DNS system. A peer-to-peer system can also be used as the querying method for a decentralised DNS. The modified DNS server [0] software is managed by volunteers in a peer-to-peer system, and no central authority may interfere with the TLD's operation [3]. The TLD.bit is Namecoin's domain's first and only TLD. The Namecoin protocol includes instructions for registering a new domain or modifying an existing one.

II. HISTORY OF NAMECOIN

A debate regarding a fictitious system named BitDNS and generalising bitcoin began in September 2010 on the Bitcoin Talk forum. In December 2010, Gavin Andresen and Satoshi Nakamoto engaged in the BitcoinTalk forum to promote the concept of BitDNS, and a BitDNS prize was announced. On the subject, a post about implementation was made[2]. On block number 19200 Namecoin implemented merged mining upgrade, enabling miners to mine both Bitcoin and Ethereum Namecoin at same time, rather than having to choose between the two. This solved the problem of miners switching from one blockchain to another as the profitability of the former improved [4].

NameID was introduced two years later, in June 2013. NameID is a tool for linking profile information to identities on the Namecoin blockchain, as well as an OpenID provider for using Namecoin identities to log into existing websites. The primary site is complemented with an open protocol for password-less authentication with Namecoin IDs, as well as a free software implementation and a Firefox plugin. Michael Gronager, the main creator of libcoin, discovered a security flaw in the Namecoin protocol in October 2013, allowing for the modification of foreign names. Except for bitcoin.bit as a proof-of-concept, it was effectively patched in a short timescale and was never exploited. In a published study, ICANN cited Namecoin as the most well-known example of DNS control and privacy distribution. Only 28 of the 120,000 domain names registered on Namecoin were used according to a 2015 analysis.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IX Sep 2022- Available at www.ijraset.com

On the OpenNIC mailing list in December 2018, a proposal was made to drop support for Namecoin.bit domains, citing Spamhaus' (and by extension other antivirus software) blocking of several of their servers due to malware spread from some.bit domains, as well as concerns about potential child pornography. There was no agreement reached during the voting. Due to security concerns raised by Namecoin and PRISM Break developers, OpenNIC was recommended to discontinue support for the.bit namespace in the same month.

OpenNIC voted again in July 2019 to delete the.bit namespace, citing "many issues with support for NameCoin domains" and growing enmity between the two projects. The vote was successful. Jeremy Rand, a Namecoin creator, praised the action, congratulating OpenNIC and calling it the "correct choice."

III. RESEARCH METHODOLOGY

We emphasise the following two questions in this essay. First, does the development of the namecoin network over time obey the densification law? Second, how do namecoin and bitcoin vary from one another in terms of the way their networks have evolved over time? In specifically, given that namecoin is a descendant of bitcoin, do they follow the same pattern? Information on the namecoin blockchain may be found on the website http://webbtc.com. The next step after obtaining the database dump is to put it in a database and extract the data required for the study. All of the blockchain's data, including block ids, transaction ids, input addresses, output addresses, and the amount of namecoin used in each transaction, are included in the original raw data. We used the networkit and igraph packages in r to study the namecoin network after creating the network graph with the transaction data that was pulled from the database. The major objective of using such tools was to identify the network's evolving patterns and features. The data from the namecoin blockchain utilised in this study spans the years 2011/04/17 to 2014/10/13. The information is gathered and evaluated over the course of seven six-month intervals in order to track the network's expansion. Each namecoin address is represented by a node in the network, while interactions between addresses are represented by edges.

A transaction with two input addresses and three output addresses, for instance, creates six edges on the network. Since the nodes don't have a connection to any other nodes, they are not included in the network since their addresses have never been used as input in a transaction. The number of edges, the number of nodes, and the average degree of the network are a few of the crucial features we must look at in order to understand the pattern of how the network grows. Understanding the network's structure also requires knowledge about the biggest connected component (lcc) and the size of the communities. As a result, we also consider the number and size of the community, as well as the proportional size and diameter of the lcc.

IV. DESCRIPTION OF NAMECOIN

A decentralised peer-to-peer network mints and maintains Namecoin. To avoid theft, Namecoin transactions need the account holder's digital signature, and each transaction is recorded in the block chain, which is an append-only hash chain [5]. Any participant (known as miners) can add new transactions to the block chain, and in exchange for doing so, they get freshly minted Namecoin money (NMC) and transaction fees from the transactions. Extensions to the block chain require a proof-of-work process that rate-limits the process (to about one extension every ten minutes), allowing for a consistent inflation rate, plenty of competition among participants to extend the block chain, and enough time to obtain and verify the block chain's history for new participants. Informally, Namecoin's proof-of-work mechanism is designed to keep the block chain's following two key properties:

1) The sequence and validity of transactions in the block chain are finally agreed upon by all parties.
2) Anyone (for a charge) can publish a transaction, which will be checked and, if legitimate, added to the block chain within a modest limited delay.

V. TECHNICAL DETAILS OF NAMES

In this subsection and the next, we present the details of Namecoin, separating the technical solution from the design choices of the mechanism. The feature that separates Namecoin from Bitcoin is that Namecoin is a namespace and can be used to store name/value pairs that can be stored on the blockchain and exchanged between individuals. This registration is done using three Namecoin-specific script operations: NAME_NEW, NAME_FIRSTUPDATE, and NAME_UPDATE. To understand the registration process, we believe it will be helpful to go through the name registration process. NAME_About. To get started, users will need to choose a coin to turn into a token (or special coin) that represents its name and value which can be changed by anyone who owns the token. The next step for name registration is to do a transaction using the

NAME_NEWscript operation in a transaction that sends tokens from one of their addresses to anotherUsing NAME_NEW, a user can show interest in the name of a name/value pair by posting a commit hash of the desired name in the transaction's scriptPubKey.

Why do users publish names in hash first, instead of than in plaintext, is to prevent pre-running. The NAME_NEW operation acts as a signal in the block chain for the name parser to indicate that the script is next. -PubKey will be the hash to name attachment.
NAME_FIRSTUPDATE. Then, and while waiting for 12 or more blocks against the block containing the NAME_NEW transaction (to ensure that the blockchain reaches consensus on the NAME_NEW transaction), the same user can use the output of the NAME_NEW transaction as input to the NAME_FIRSTUPDATE transaction. When done, this will associate the selected name with the value selected by the user [13]. Similar to NAME_NEW, NAME_FIRSTUPDATE allows data to be published to the blockchain as part of the scriptPubKey of a particular transaction. To create a NAME_NEW transaction, the user selects, as input, the output of the NAME_NEW transaction. They will then use another address they control as the exit for the transaction. The ScriptPubKey of this transaction will contain NAME_FIRSTUPDATE, the desired name, the random number used in the NAME_NEW hash commit, and the first value of the name. 2 For this transaction to be valid, the miner will verify that the name and nonce provided are indeed the commit hash in the appropriate NAME_NEW transaction. The output of this transaction now contains a token representing a name/value pair for name and value, and anyone who can unlock and use the output can use the last new operation,
NAME_UPDATE. The third and last new operation in Namecoin is the NAME_UPDATE operation. Again, the arguments for this operation (name and newValue) are stored in the scriptPubKey of a particular transaction. This transaction must output either NAME_FIRSTUPDATE or NAME_UPDATE with the same name. This has three uses: update, renew, and rename. If the user wants to modify the value associated with a certain name, he updates the name with this operation, providing a new value [12]. If the name is subject to expiration, as is the case with Namecoin, this operation can also be used to renew the name by providing a new value that is the same as the old value. In both cases, the user will use the address they control as a result of the transaction. The final reason to do a NAME_UPDATE transaction is to exchange special coins with other users. In this case, the user will output another user's address instead of their own. Once the transaction is settled, other users will have control over the special coin and can modify the value at will. Since name ownership is linked to ownership of special coins, if the buyer pays for the name with Namecoins, the exchange between the payment and the name can be atomic (meaning they happen within same transaction and that transaction or the other is only valid if the other is also valid).

VI. RELATED WORK

The first cryptocurrency to attempt to merge blockchain with domain name service was Namecoin. In order to eliminate domain name censorship and facilitate the spread of network information, Namecoin primarily focuses on the DNS flaws that now exist and the development of a decentralised DNS system using blockchain. The POW consensus process is used by Namecoin to create a new blockchain, similar to Bitcoin. Namecoin is equivalent to the.bit domain name, which offers a comparable.com service, but.bit domain names are permanently recorded on the blockchain and can only be managed by the owner. Virtual chain technology plus the addition of a few Blockstack servers make it such that Bitcoin nodes cannot detect the presence of Blockstack servers. Transactions involving domain names are processed by Blockstack servers, and the efficient handling of transactions is ensured by the robust Bitcoin network. In addition, Blockstack takes into account the constraints of blockchain storage, builds a four layer architecture, and adds third party storage to relieve the strain on blockchain nodes, although it still appears a little confusing. On the other side, Bitcoin's underlying blockchain places restrictions on Blockstack's performance. Currently, Bitcoin produces blocks of 1MB in size every 10 minutes on average, which makes Blockstack ineffective. In order to eliminate single centre nodes and encourage additional organisations to engage in the management and upkeep of domain name services, this article presents ConsortiumDNS, which is based on consortium chain.

VII. WHAT IS DIFFERENCES BETWEEN BITCOIN, LITECOIN AND NAMECOIN

A decentralised electronic ledger can eliminate the counterparty risk posed by a centralised third party. Theoretically, every imaginable virtual transaction might be decentralised on a blockchain, avoiding the expenses and hazards of dealing with a governing authority. The main issue is whether to construct I a separate network based on a unique consensus process or (ii) a protocol on top of the Bitcoin protocol. The following is an example of each of the two scenarios using the platforms Namecoin and Litecoin: Like Litecoin, Namecoin is a different cryptocurrency (i.e. Altcoin).However, the distinction between Namecoin and Litecoin is that the Namecoin blockchain is based on an independent protocol rather than directly on the Bitcoin protocol, even if it uses the same algorithm as Bitcoin. In contrast, the Litecoin blockchain is a separate common network that is built on a unique protocol with the aim of accelerating transactions and improving the cost and resource efficiency of mining.

The average transaction confirmation time in Litecoin is 2.5 minutes. It typically takes 10 minutes to use Bitcoin. Another distinction is the planned supply limit for coins. 84 million coins are planned for Litecoin, compared to 21 million for Bitcoin.

VIII. APPLICATIONS

Namecoin's creators suggest that this experimental money might have a variety of functions and applications. The developers seek to defend free speech rights online first and foremost by making the web more resistant to repression. Namecoin tries to do this in a variety of ways. It may be used to associate identifying information with multiple identities defined by the user, such as email addresses, Bitcoin addresses, or specified keys. It may also be used to provide decentralised certificate validation for TLS (HTTPS). To produce human-meaningful Tor.onion domains, Namecoin may be employed in Tor and dark web capabilities. Cryptocurrency and its underlying technology might be used for file signatures, safeguarding voting procedures, notary services, and providing evidence of existence for persons and businesses in the future.

Namecoin is a registration and transfer mechanism for key/value pairs based on Bitcoin technology. As a result, Namecoin may be used to securely store and transfer arbitrary names or keys. It can also save information about these people's names. These names are difficult to censor or confiscate because of their ties to the Namecoin network, making them resistant to outside intervention. Furthermore, Namecoin's creators state that lookups do not produce network traffic. As a consequence, Namecoin now has better privacy capabilities.

IX. RESULT & DISCUSSIONS

All of the threats listed in RFC 3833 can be countered depending on how Namecoin is used. All threats are mitigated when the blockchain is kept locally. Clients must, however, revert to the old DNS protocol when the blockchain is stored on a distant system. Packet eavesdropping, ID guessing and query prediction, betrayal by trusted servers, denial of service, and wildcard matching attacks are all now conceivable [14]. Domain name denials that are authenticated can no longer be believed. Because of Namecoin's distributed architecture, it can provide censorship resistance. Each node is the same as the others. When the blockchain is kept locally, there are no plain text queries that must be sent over the internet, ensuring privacy. Namecoin also promises to be quicker, however this has yet to be proven.

X. FUTURE SCOPE

Namecoin appears to have a lot of potential, but it still needs a lot of work before it can be utilised on the Internet. When the blockchain is utilised more often, it will contain a large amount of data, making it difficult to store locally. In the event that the blockchain must be kept on a distant server, standard DNS searches will be used, which are vulnerable to assaults. The DNS system must be replaced by another protocol to protect against all of the vulnerabilities described and to provide the anonymity that Namecoin can provide when a local blockchain is available. Existing protocols such as DNSCurve might perhaps be used to encrypt traffic and ensure packets cannot be replayed. However, there may be better options, such as developing a whole new remote access protocol [8].

Another aspect of Namecoin's performance that has not been investigated is how it compares to DNS. We believe it is possible that Namecoin lookups are substantially quicker than DNS lookups. Especially when the blockchain is kept locally and queries do not need to be sent over the Internet [9]. We won't know if our expectations are accurate unless we take adequate measurements. There are several factors to consider (such as blockchain size, cache, lookup methods, and processing power), making it conceivable to devote an entire project to the performance comparison.

XI. CONCLUSION

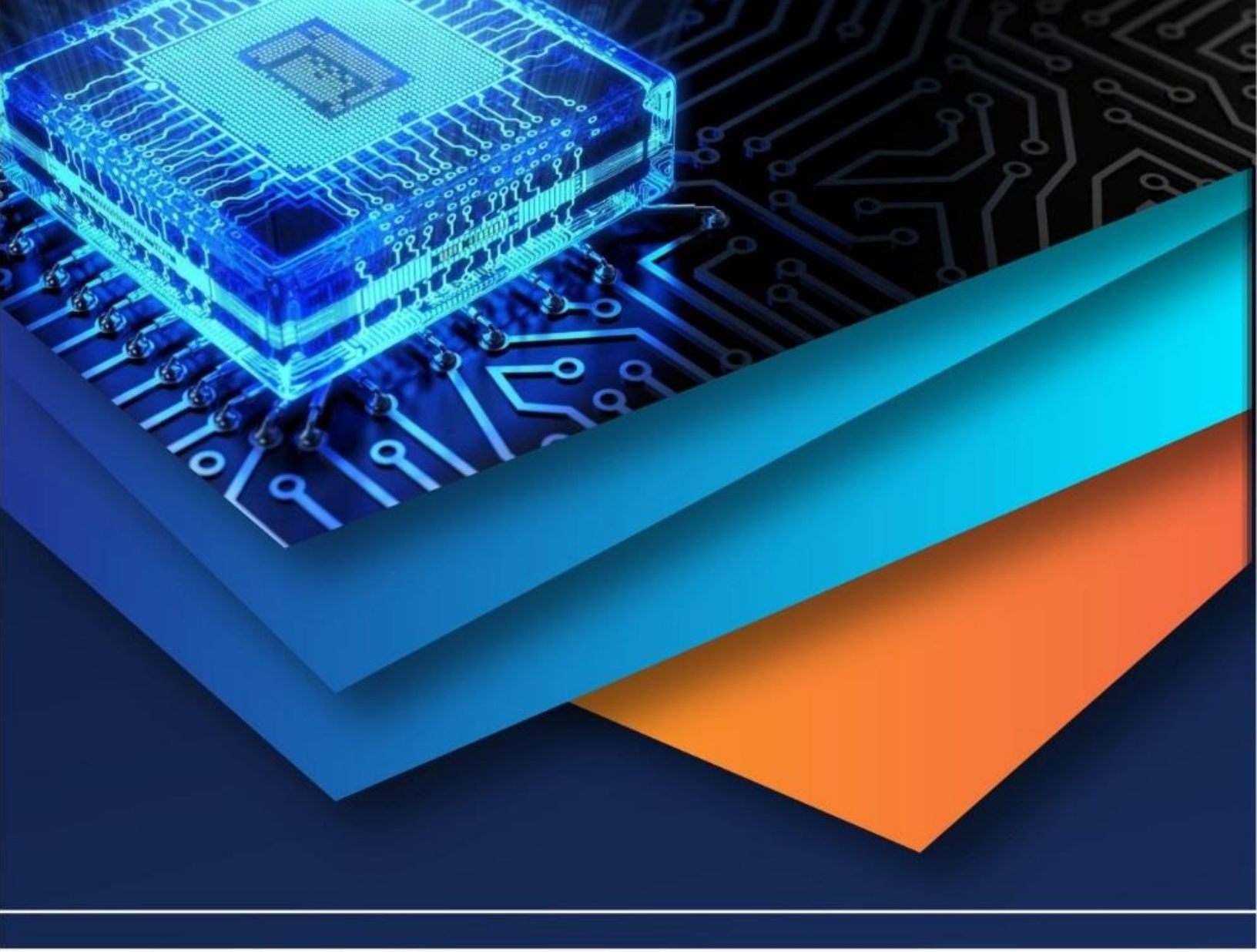
Since Namecoin is a distributed system, all of the load (queries, registrations, and data delivery) will be dispersed over all nodes in the network. This P2P method assures that all nodes only use a little amount of resources, rather than a large number of servers. The Domain Name System (DNS) is a decentralised system with a hierarchical structure. The root name servers (at the top of the tree) are under a lot of stress, whereas farther down the tree, fewer resources are required [10].

XII. ACKNOWLEDGEMENT

Alisha Gupta, Bhushan Chaudhary and Pratibha Dwivedi are thankful to TCET for providing a beneficial platform to the students in the form of RBL and conceiving interest and awareness about writing, presenting and publishing articles.

REFERENCES

[1] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," Applied Innovation, vol. 2, pp. 6–10, 2016.
[2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
[3] coldfustion, "Why blockchain matters more than you think!" Sep 2017. [Online]. Available: https://www.youtube.com/watch?v=sDNN0uH2Z3o
[4] "The great chain of being sure about things," Oct 2015. [Online]. Avail-able: https://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable
[5] T. McConaghy, R. Marques, A. Müller, D. De Jonghe, T. McConaghy, G. McMullen, R. Henderson, S. Bellemare, and A. Granzotto, "Bigchaindb: a scalable blockchaindatabase," white paper, BigChainDB, 2016.
[6] S. Wilkinson, T. Boshevski, J. Brandoff, and V. Buterin, "Storj a peer-to-peer cloud storage network," 2014
[7] Jacobs, F. (2014). Providing better confiden- tiality and authentication on the Internet using Namecoin and MinimaLT (arXiv:1407.6453v1). Accessed from http://arxiv.org/abs/1407.6453
[8] Melin, T., & Vidhall, T. (2014). Name- coin as authentication for public-key cryptography (LIU-IDA/LITH-EX-G– 14/067–SE). Accessed from http://liu.diva-portal.org/smash/record.jsf?pid=diva2%3A730 344&dswid=-2203
[9] Atkins, D. and Austein, R. (2004). RFC 3833 - Threat Analysis of the Domain Name Sys- tem (DNS). [online] Tools.ietf.org. Available at: https://tools.ietf.org/html/rfc3833 [Accessed 7 Jan. 2016].
[10] Wiki.namecoin.info, (n.d.). Namecoin Wiki - FAQ. [online] Available at: https://wiki.namecoin.info/index.php?title=FAQ [Accessed 13 Jan. 2016].
[11] Antonopoulos, A. (2014). Mastering Bitcoin. Se- bastopol, California: O'Reilly.
[12] Weaver, N., Kreibich, C., Nechaev, B. and Paxson, V. (2002). Implications of Net- alyzrs DNS Measurements. [online] The ICSI Networking and Security Group. Available at: http://www.icir.org/christian/publications/2011- satin-netalyzr.pdf [Accessed 29 Jan. 2016].
[13] Wilcox-O'Hearn, Z. (2006). Names: Decentral- ized, Secure, Human-Meaningful: Choose Two. [online] Shoestringfoundation.org. Available at: http://shoestringfoundation.org/ bauerm/names/ distnames.html [Accessed 18 Jan. 2016].
[14] Cohen, B. (2015). What is One- name?. [online] Onename. Available at: https://onename.zendesk.com/hc/en- us/articles/202288932-What-is-Onename- [Accessed 14 Jan. 2016].
[15] Cheshire, S. and Krochmal, M. (2013). RFC 6761 - Special-Use Domain Names. [online] Tools.ietf.org. Available at: https://tools.ietf.org/html/rfc6761 [Accessed 28 Jan. 2016].
[16] Grothoff, C., Wachs, M., Wolf, H., Appel- baum, J. and Ryge, L. (2015). Draft: Special- Use Domain Names of Peer-to-Peer Systems. [online] Internet Engineering Task Force. Avail- able at: https://www.ietf.org/archive/id/draft- grothoff-iesg-special-use-p2p-names-04.txt [Ac- cessed 28 Jan. 2016].
[17] Luke A Walker. Icann's uniform domain name dispute resolution policy. Berk. Tech. LJ, 15:289, 2000.
[18] William L Silber. Marketmaker behavior in an auction market: an analysis of scalpers in futures markets. The Journal of Finance, 39(4):937–953, 1984.
[19] John R Ottensmann. Urban sprawl, land values and the density of development. Land economics, pages 389–400, 1977.
[20] Atila Abdulkadiroglu and Tayfun Sönmez. Match- ing markets: Theory and practice. In Advances in Economics and Econometrics (Tenth World Congress), pages 3–47, 2013.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY