A Comprehensive Study on Namecoin

Alisha Gupta, Bhushan Chaudhary and Pratibha Dwivedi

February 8, 2022

A Comprehensive Study on Namecoin

Alisha Gupta
Information Technology
Thakur College of Engineering & Technology
Kandivali East, Mumbai
alishacamb@gmail.com

Bhushan Chaudhary
Information Technology
Thakur College of Engineering & Technology
Kandivali East, Mumbai
bhushanchaudhary3333@gmail.com

Pratibha Dwivedi
Information Technology
Thakur College of Engineering & Technology
Kandivali East, Mumbai
dwivedipratz@gmail.com

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 anybody can now exist thanks to the introduction of a decentralised DNS system. A peer-to-peer system also serves as the querying method for a decentralised DNS. Volunteers manage the modified DNS server software in a peer-to-peer system, and no central authority may meddle in the TLD's functioning [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 hypothetical system named BitDNS and generalising bitcoin began in September 2010 on the BitcoinTalk forum. In December 2010, Gavin Andresen and Satoshi Nakamoto joined the BitcoinTalk forum to advocate the notion of BitDNS, and a prize for BitDNS implementation was posted on the topic. On block 19200, Namecoin implemented the merged mining upgrade, allowing miners to mine both Bitcoin and Namecoin at the same time, rather than having to pick between the two. This resolved the issue of miners jumping from one blockchain to the other when the former's profitability 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. 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. 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:

- The sequence and validity of transactions in the block chain are finally agreed upon by all parties.
- 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.

IV. 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 [6]. Furthermore, Namecoin's creators state that lookups do not produce network traffic. As a consequence, Namecoin now has better privacy capabilities.

V. 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 [7]. 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.

VI. 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.

VII. 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].

VIII. 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.

IX. REFERENCES

[1] Jacobs, F. (2014). Providing better confidentiality and authentication on the Internet using Namecoin and MinimaLT (arXiv:1407.6453v1). Accessed from http://arxiv.org/abs/1407.6453

[2] 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%3A730344&dswid=-2203

[3] 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].

[4] Wiki.namecoin.info, (n.d.). Namecoin Wiki - FAQ. [online] Available at: https://wiki.namecoin.info/index.php?title=FAQ [Accessed 13 Jan. 2016].

[5] Antonopoulos, A. (2014). Mastering Bitcoin. Sebastopol, California: O'Reilly.

[6] 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].

[7] Wilcox-O'Hearn, Z. (2006). Names: Decentralized, Secure, Human-Meaningful: Choose Two. [online] Shoestringfoundation.org. Available at: http://shoestringfoundation.org/ bauerm/names/ distnames.html [Accessed 18 Jan. 2016].

[8] 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].

[9] 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].

[10] Grothoff, C., Wachs, M., Wolf, H., Appelbaum, 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].