Proceedings of the 2nd International Conference on Software Engineering and Machine Learning
DOI: 10.54254/2755-2721/74/20240422

Ensuring information security and stability: The application of blockchain in naming system

Zerong Liu

School of Information Science and Engineering, East China University of Science and Technology, Shanghai, 200000, China

22013404@mail.ecust.edu.cn

Abstract. In recent years, network information security and stability problems have emerged one after another, and people's personal privacy and property security are being threatened. A large part of these problems are caused by two major characteristics of traditional DNS—insecurity and instability. Therefore, this article aims to explore a new internet naming system—the Blockchain Naming System—to address the current issues of internet information security and stability—especially the problems caused by the traditional DNS system. This article adopts scientific research methods such as literature survey, comparative research, experimental exploration, analogy research, and model building. By analyzing the current situation, studying the feasibility of the blockchain naming system, and comparing its advantages and disadvantages with the traditional DNS system, it is not difficult to conclude that this new blockchain naming system has huge potential. It can not only ensure stability and security but also contribute to other fields.

Keywords: Lockchain, DNS, Security, Stability.

1. Introduction

In the contemporary digital age, the Internet has become deeply integrated into our daily lives and business activities. However, concerns surrounding network information security and stability have gained prominence, posing significant threats to individual privacy and property security. Two major drawbacks of the traditional Domain Name System (DNS) — insecurity and instability — have contributed substantially to these challenges. This research endeavors to explore a novel internet naming system: the Blockchain Naming System, to address current issues about internet information security and stability, particularly those stemming from the conventional DNS system.

Regarding this issue, similar ideas have been proposed in the scientific field, such as Blockstack: A global naming and storage system secured by blockchains; Bitforest: a portable and efficient blockchain-based naming system; Namecoin, etc. These ideas discuss the prominent role that blockchain plays in certain aspects of the naming system, such as the decentralization of Bloclstack and Namecoin, the scalability of Bitforest, etc [1-2]. But in this article, we will not only discuss and analyze the security and stability characteristics of the blockchain naming system and the reasons for their emergence but also discuss how these characteristics can contribute to other fields, such as the Internet of Things and information confidentiality.

DOI: 10.54254/2755-2721/74/20240422

The traditional DNS system grapples with significant issues related to security and stability, including single points of failure, a lack of security validation mechanisms, and susceptibility to malicious attacks. These concerns have given rise to the demand for a more reliable and secure internet naming system.

This study primarily revolves around the exploration of the Blockchain Naming System as a potential solution. Specifically, we will delve into the architecture, functioning, and security features of the Blockchain Naming System. We will probe the following key research questions in depth:

How does the Blockchain Naming System ensure the security and stability of network information?

What differentiates the performance and scalability of the Blockchain Naming System from the traditional DNS system?

How does the Blockchain Naming System address potential security threats and attacks?

This study will employ a variety of scientific research methods, including literature surveys, comparative research, experimental exploration, analogy research, and model construction. Through these methods, we will thoroughly analyze the current landscape, assess the feasibility of the Blockchain Naming System, and compare its strengths and weaknesses with those of the traditional DNS system.

This research aims to provide novel insights and solutions for addressing contemporary issues surrounding internet information security and stability. If the Blockchain Naming System is found to possess significant potential, it can not only enhance network stability and security but also contribute to advancements in other fields. Additionally, this study will offer predictions and recommendations for future developments to foster the well-being and sustainable growth of the Internet ecosystem.

2. Situation Analysis

2.1. Definition of Naming System (DNS)

DNS (Domain Name System) is a system used to translate domain names into IP addresses. On the internet, every device (such as servers, computers, smartphones, etc.) has a unique IP address composed of a series of numbers, which is not easy to remember for humans. Therefore, DNS was created to allow us to access websites and network resources using more human-friendly, easier-to-remember domain names [3].

Here is a brief description of how the DNS mechanism works:

When a user enters a domain name, such as "www.example.com," into a web browser, the browser initiates a DNS resolution request. This request is sent to a DNS server, which begins by checking its local cache database to determine if it already has the corresponding IP address for the domain name. If the IP address is not found in the cache, the DNS server commences a recursive search, reaching out to other DNS servers to locate the correct IP address.

Once the DNS server successfully identifies the IP address, it promptly returns this information to the browser. Armed with the IP address, the browser proceeds to establish contact with the target server by sending a request to the identified IP address. The target server then responds to the browser's request by transmitting the website's content.

Finally, the browser, upon receiving the data from the server, skillfully presents the website content, making it accessible and viewable to the user. This entire process ensures the seamless retrieval and display of web pages as users navigate the internet [4].

Thanks to DNS, people can use easy-to-remember names to access websites instead of having to memorize complex IP addresses.

2.2. The Current Situation of DNS

2.2.1. Situation 1: Unsafe. In recent years, online frauds have emerged in an endless stream, seriously threatening our information security. DNS hijacking is one of the common methods.

DNS hijacking is a malicious attack method in which an attacker redirects users to a malicious website with a URL different from the expected one by tampering with the response of the DNS server,

DOI: 10.54254/2755-2721/74/20240422

changing the DNS settings of the local host, or directly attacking the DNS tunnel. Such attacks could be used to spread malware, conduct phishing, or collect personal information [5].

Well, people might compare DNS to a phone book. When you want to visit a website, your computer will look up this "phone book", find the "phone number" (that is, the IP address) of the website, and then dial it. Through this method, you can talk with this website.

DNS hijacking is like someone deliberately changing a wrong number in your phone book. When you try to call a friend's number, you're calling a stranger. Online, means that when you try to visit a familiar site, you may be redirected to a similar-looking site that is malicious. This fake website might try to steal your information or make you download harmful software.

2.2.2. Situation 2: Unstable. The Domain Name System (DNS) is a critical component of the Internet, but its centralization presents inherent vulnerabilities that can lead to network instability. This centralization primarily stems from the reliance on a central server or a limited set of servers to manage and coordinate the mapping of domain names to IP addresses. This centralized architecture can result in a single point of failure, as all the surrounding nodes in the network depend on these central servers for DNS resolution.

In the event of a server failure, whether due to technical issues, cyberattacks, or other disruptions, the consequences can be significant. When the central server is compromised, all the connected nodes lose their ability to resolve domain names to IP addresses. This means that websites, services, and applications become inaccessible to users, causing disruptions and downtime. The impact of such an outage can be especially severe when considering the critical role of DNS in facilitating communication and information access on the internet.

3. Problem resolution

3.1. Definition of Blockchain

A blockchain is a distributed database that uses cryptography to link and secure records. Each block includes a series of transactions, which are linked together with the previous block through the hash value, thus forming a chain structure [6].

You can think of the blockchain as a public ledger, each page (or "block") records many transaction details, and these pages are connected in chronological order to form a continuous chain.

In the blockchain network, the process begins with users creating transactions via a network application or wallet, and these transactions are initially subject to verification by other nodes within the network. This verification encompasses checking the transaction's legitimacy, including the availability of sufficient funds for its completion. Once verified, the transaction joins a pool of pending transactions, where miners or validators select and package them into a block.

The newly formed block undergoes verification by other network nodes to ensure the legitimacy of all contained transactions and compliance with network rules. Upon successful verification, the block is seamlessly added to the blockchain, which serves as a continually expanding public ledger of transaction records. In many blockchain networks, such as Bitcoin, the node responsible for adding a new block to the chain receives a reward, often in the form of cryptocurrency.

To maintain consensus across the network regarding the current state of the blockchain, blockchain networks rely on a consensus mechanism, with common examples being Proof of Work (PoW) and Proof of Stake (PoS). Furthermore, the decentralized nature and encryption technology of blockchain providesprovides a high level of security, rendering data added to the chain both irreversible and resistant to unauthorized alterations. Any attempts to modify existing blocks are swiftly detected and rejected by the network, ensuring the integrity and immutability of the blockchain's transaction history [7].

This mode of operation of blockchain technology ensures data transparency, security, and immutability, making it an ideal choice for financial services, supply chain management, proof of property rights, and many other applications.

DOI: 10.54254/2755-2721/74/20240422

3.2. Characteristics of Blockchain

Through the description of the working process of blockchain, people can easily conclude that blockchain has the following characteristics:

First and foremost, it operates on the principle of decentralization, which means there is no central authority or server that governs the network. Instead, the network is distributed across numerous nodes, each with its copy of the blockchain, ensuring that no single entity has ultimate control, thus promoting trust and security.

Secondly, blockchain offers transparency as a core feature. This means that all participants in the network can access and view an entire, unaltered copy of the blockchain, which includes all transaction records and data. This transparency not only fosters trust but also allows for public scrutiny, reducing the potential for fraudulent or malicious activities.

Furthermore, blockchain technology ensures the permanence of data. Once information is recorded on the blockchain, it becomes exceedingly challenging, if not practically impossible, to modify or delete. This immutability is a result of cryptographic hashing and consensus mechanisms, which safeguard the integrity of the data and make it resistant to tampering.

Lastly, the consensus mechanism is a pivotal component of blockchain systems. To add new data to the blockchain, necessitates the consent and agreement of the entire network. This consensus ensures that only valid and verified transactions are added, enhancing the overall trustworthiness and security of the blockchain network by preventing unauthorized or fraudulent data from being incorporated [8].

These characteristics allow people to record transactions openly and securely, without the need for a central authority to store and verify them.

3.3. The Combination of Blockchain and Naming System

Since the blockchain can guarantee the security of information, people might as well store the things stored in the DNS phone book (the correspondence between network names and addresses) in the blockchain to form a globally shared and transparent phone book [9].

Whenever someone wants to modify something inside, it needs the consent of the majority; and once modified, it is difficult to delete.

This is the prototype of the blockchain naming system, which can achieve the same function as DNS and is more secure than it.

The author wrote a simple Python program to build a blockchain and store the corresponding relationship between IP and network name, realizing the construction of a blockchain naming system. The key components of the code are:

Block Class (Block):

- Represents a block in the blockchain.
- Attributes include index, timestamp, data (used for storing named records), previous_hash, and hash (generated based on block attributes).
- Method hash_block computes the hash value for the block.

Blockchain Class (Blockchain):

- Represents the entire blockchain.
- Attribute chain is a list of blocks.
- Method create_genesis_block initializes the blockchain with a genesis block.
- Method add_block adds a new block to the blockchain, linking it to the previous block.

Blockchain Initialization and Data Addition:

- An instance of the Blockchain class is created: blockchain = Blockchain().
- Two blocks are added to the blockchain using the add_block method, each containing a named record (domain name and corresponding IP address).

Record Retrieval (find_domain Function):

- The find_domain function is defined to retrieve the IP address associated with a given domain name.

DOI: 10.54254/2755-2721/74/20240422

- It iterates through the blocks in the blockchain (excluding the genesis block) and checks if the block's data contains the specified domain name.
- If a match is found, the corresponding IP address is returned; otherwise, None is returned.

Execution and Result:

- The find_domain function is used to find the IP address for the domain "google.com."
- The result is printed: "The IP address for google.com is 209.85.128.0."

In summary, the program demonstrates the creation of a basic blockchain to store named records (domain names and IP addresses). It establishes a clear structure with the Block and Blockchain classes, allowing the addition of blocks with named records. The find_domain function facilitates the retrieval of IP addresses based on domain names, and the provided example successfully retrieves the IP address for "google.com." The design is modular and follows a standard blockchain structure for maintaining a secure and linked record of information.

3.3.1. Code Running Result. The IP address for google.com is 209.85.128.0.

While this program simplifies many of the complex aspects of blockchain technology, it provides a clear example of how blockchains can be used to store and retrieve named information.

In addition, for confidential internal networks, people can also add a blockchain-implemented access record system based on the use of the blockchain naming system. This way, even if someone indeed tampers with the information recorded in the blockchain naming system (although the likelihood of this happening is extremely low, see part 3 for details), their access information will be very difficult to erase, because the data within such an access record system maintains the same level of security and immutability as the blockchain. This kind of system can also effectively prevent leaks and facilitate our reviews.

The author also wrote a Python program to do it. The code defines a simple blockchain structure using Python classes, including two main classes: Block and Blockchain. It also includes a mining process.

Block Class:

__init__ method:

- Initializes a block with properties like index, timestamp, transactions, previous hash, nonce.
- Computes the hash using the **compute_hash** method.

compute_hash method:

- Converts block properties to a string and calculates the SHA-256 hash.
- The hash is crucial for blockchain integrity.

mine method:

- Mines a block by finding a hash with a specific difficulty level.
- Uses a nonce to alter the hash until the desired pattern is achieved.

Blockchain Class:

__init__ method:

- Initializes the blockchain with a genesis block and an empty list for pending transactions.

create_genesis_block method:

- Creates the genesis block, representing the start of the blockchain.

get_last_block method:

- Returns the last block in the chain.

verify_transaction method:

- Checks if a transaction has required fields.

add_transaction method:

- Validates and adds transactions to the pending list.

DOI: 10.54254/2755-2721/74/20240422

mine_block method:

- Creates and mines a new block using Proof of Work.
- Adds the block to the chain and clears pending transactions.

Mining Process:

Involves hash preparation, calculation, verification, and nonce adjustment.
Proof of Work ensures security and integrity.
Difficulty level adjusts the mining process.

Here is its main program:

Creates a transaction representing an access request.
Creates a blockchain instance.
Adds the access request transaction to the blockchain.
Mines a new block to confirm transactions.
Prints blockchain information to view recorded access requests.

The code defines a blockchain with a block structure, implementing Proof of Work for mining. The blockchain manages transactions, ensures integrity through hash functions, and uses a difficulty level for mining.

3.3.2. Code Running Result.

{'index': 0,
'timestamp': 1692810044.116212,
'transactions': [],
'previous_hash': '0',
'nonce': 0,
'hash': 'fbb10639f0f71c2f013c6405e6bb2af5659d73a162bfed054668fc6964ffe440'}

{'index': 1,
'timestamp': 1692810044.1164467,
'transactions': [{
'user': 'Alice',
'resource': 'file.txt',
'action': 'read',
'timestamp': 1692810044.1161497}],
'previous_hash': 'fbb10639f0f71c2f013c6405e6bb2af5659d73a162bfed054668fc6964ffe440',
'nonce': 273808,
'hash': '0000e98990b3221ca5c1c5e7b0c16a4940fa83e6fec49b75bc2cd330bf44ef82'}

It successfully logs access events. This means that the event is permanently stored on the blockchain and can be seen and reviewed by anyone.

3.4. Advantages and Disadvantages of Blockchain Naming System

As you can see, the experiment above shows the possibility of building a blockchain naming system. So, is it possible for this system to replace the existing DNS system? To answer this question, people need to analyze the pros and cons of this system.

3.4.1. Advantage 1: Safety. First of all, due to the decentralization of the blockchain, the blockchain naming system does not require a central server like DNS, and domain name information is stored on the distributed blockchain network. This makes it impossible for criminals to attack servers to create hijacking like DNS.

Secondly, because of the hash connection, even if the criminal successfully hijacks some nodes, it is almost impossible to modify the existing information on it unless he destroys all subsequent blocks. Similarly, because the blockchain has a consensus mechanism, it is not easy to add something bad unless he has the consent of all nodes.

DOI: 10.54254/2755-2721/74/20240422

Finally, because of the transparency and permanence of the blockchain, even if criminals successfully rewrite the above data, the data will be permanently stored on the blockchain for everyone to see. This facilitates the police to track criminals.

3.4.2. Advantage 2: Stability and Robustness. This advantage is also provided by the decentralization of the blockchain. Since the data is no longer centrally stored on the central server, even if some nodes fail, the data on the blockchain can still be accessed. This improves system stability and reliability.

Such advantages are especially prominent in the Internet of Things. The Internet of Things, like the Internet, also requires the link of matching object names (or identifiers) with addresses (such as IP addresses). However, the Internet of Things requires stability and reliability in some ways more than the Internet [10].

For example: Critical infrastructure: Many IoT devices are used in critical infrastructure such as energy, healthcare, and traffic management. In these cases, any failure can have serious consequences, such as power outages, malfunctioning medical equipment, or traffic jams.

Real-time response: Some IoT applications require real-time or near-real-time response, such as industrial automation and self-driving cars. In these cases, availability and robustness are of paramount importance, as failures can directly endanger human life and safety.

Dispersed environment: IoT devices are often spread across a wide range of geographic locations, covering a variety of environments and conditions. Decentralized systems are better suited to this diverse and widely distributed environment. Just like supermarket chains can configure their warehouses according to the needs of each region.

3.4.3. Disadvantages and challenges. Even though blockchain naming systems have many advantages compared to traditional DNS, there are still many disadvantages and challenges in putting such systems into practical applications [11].

Technical challenges: Refactoring the entire DNS architecture with blockchain is a massive engineering task involving many technical and implementation challenges.

Performance issues: Compared with traditional databases, the read and write speed of blockchain is slower. DNS needs to resolve domain names quickly, and blockchain may not be suitable for handling a large number of instant queries.

Compatibility: Existing Internet infrastructure and applications are built around the current DNS system. Replacing DNS with blockchain may require massive changes and redesigns.

4. Conclusion

In summary, the research underscores the advantages of the Blockchain Naming System over the traditional DNS in terms of security, transparency, and stability. It offers a promising solution to the contemporary challenges of internet information security and stability. However, it is crucial to acknowledge that the Blockchain Naming System may not serve as a direct replacement for the DNS, given the current technological and infrastructure landscape.

As things stand, the blockchain is more likely to complement or enhance the existing DNS system rather than entirely supplant it. Future breakthroughs in technology or the emergence of specific application scenarios could potentially alter this landscape, and there are indeed organizations and initiatives like ENS and Namecoin actively exploring the development of a blockchain-based naming system to replace DNS. Nevertheless, the transition from DNS to blockchain remains a formidable and complex task, and its feasibility in the real-world context remains uncertain [12].

Looking ahead, the potential applications of blockchain technology extend well beyond naming systems. It can be harnessed to manage resources, financial transactions, digital identities, and more. These application prospects are ripe for exploration by future generations of researchers and innovators. It is anticipated that blockchain's disruptive influence will continue to shape and revolutionize various domains.

DOI: 10.54254/2755-2721/74/20240422

While this research highlights the promise of blockchain technology, it is important to acknowledge its current limitations and areas for improvement. To advance this field, future research endeavors should focus on refining the interoperability between the Blockchain Naming System and the existing DNS infrastructure, addressing scalability concerns, and enhancing user-friendliness. Furthermore, collaboration between academia, industry, and government bodies is crucial to fostering a conducive environment for the evolution of blockchain technology and its integration into real-world systems.

In conclusion, the path toward blockchain replacing DNS is multifaceted and intricate. As we anticipate the future, the realm of possibilities is vast, and it is imperative to maintain an open and innovative mindset to harness the full potential of blockchain technology in reshaping the internet landscape.

References

[1] Muneeb Ali and Jude Nelson, Princeton University and Blockstack Labs; Ryan Shea, Blockstack Labs; Michael J. Freedman, Princeton University, (2016). Blockstack: A Global Naming and Storage System Secured by Blockchains. 2016 USENIX Annual Technical Conference, JUNE 22-24, 2016 DENVER, CO. [https://www.usenix.org/conference/atc16/technical-sessions/presentation/ali].

[2] Yuhao Dong; Woojung Kim; Raouf Boutaba, (2018). 2018 14th International Conference on Network and Service Management (CNSM), 05-09 November 2018. [https://ieeexplore.ieee.org/abstract/document/8584991].

[3] Wikipedia, (2023). Domain Name System. [https://en.wikipedia.org/wiki/Domain_Name_System].

[4] Cloudflare, (2023). What is DNS? | How DNS works. [https://www.cloudflare.com/zh-cn/learning/dns/what-is-dns/].

[5] Atkins, D. and Austein, R. (2004) Threat Analysis of the Domain Name System (DNS). [https://www.rfc-editor.org/rfc/rfc3833.html].

[6] Wikipedia, (2023). Blockchain. [https://en.wikipedia.org/wiki/Blockchain.

[7] OCI, (2023). What is the blockchain? [https://www.oracle.com/cn/blockchain/what-is-blockchain].

[8] Saif Al-Mashhadi and Selvakumar Manickam, (2020). A brief review of blockchain-based DNS systems. International Journal of Internet Technology and Secured Transactions, Vol. 10, No. 4: pp.420-432.

[9] Hu, W-H., Meng, A., Lin, S., Jia-Gui, X. and Yang, L. (2017) 'Review of blockchain-based DNS alternatives', Chinese Journal of Network and Information Security, Vol. 3, No. 3, pp.1–7.

[10] Shen Su, Zhihong Tian, Shuang Li, Jinxi Deng, Lihua Yin, Xiaojiang Du, Mohsen Guizani, (2021). IoT root union: A decentralized name-resolving system for IoT based on blockchain. Information Processing & Management, Volume 58, Issue 3, May 2021: pp.102553.

[11] Saif Al-Mashhadi and Selvakumar Manickam, (2020). A brief review of blockchain-based DNS systems. International Journal of Internet Technology and Secured Transactions, Vol. 10, No. 4: pp.420-432.

[12] Saif Al-Mashhadi and Selvakumar Manickam, (2020). A brief review of blockchain-based DNS systems. International Journal of Internet Technology and Secured Transactions, Vol. 10, No. 4: pp.420-432.