Blockchain: Research and Application

Zixuan Chen [1, †], Haofeng Guo [2, †, *], Yuanben Zou [3, †]

[1] College of Computer and Information, Hohai University-Nanjing-China, Nanjing, China

[2] School of Engineering & Applied Science, University of Rochester, New York State, America

[3] Beijing University of Posts and Telecommunications, Beijing, China

* Corresponding author email: hguo15@u.rochester.edu

†These authors contributed equally to this work

Abstract. Blockchain has been invented for years and it gradually become the most important technique in nowadays' internet era. Blockchain technology has been widely used in various fields, such as finance, trading, logistics, currency, etc. This paper explains and demonstrates the main algorithm and application of the blockchain. Until now, the primary applications of blockchain are mainly focus on the digital currency such as ETH. The value of blockchain, however, is not limited by only the digital currency but all the aspect within the internet. For instance, based on these years' social concern, the pandemic of COVID-19 is the most worried problem. The application of this paper concentrates on the connection between COVID-19 and blockchain. By relating the technique of blockchain, the security and data tracing of medical supplies have been insured. Moreover, the personal information security is maintained during the process of doing the covid-test and the trajectory of activity.

Keywords: Block Chain; Centralization; Decentralization; Asymmetric Encryption; COVID-19.

1. Introduction

After several years of development, blockchain technology has had many mature applications. And in today's global epidemic, blockchain also needs to play an indelible role [1]. During the epidemic, although most data records have formed a scientific and rigorous model, almost all data records are recorded independently on an individual basis. In today's globalized epidemic situation, it is very necessary to centralize and uniformly record all data to the same platform. Centralized data recording is not a safe data recording method, but with the addition of blockchain technology, with the application of decentralization and consensus mechanism, this will not be an impossible thing [2].

Based on the argument of Nabil and Chakraborty, "Information technology plays a vital role in the fight against COVID-19. It is helpful to assess the outbreak of COVID-19 pandemic, statistical classification of COVID-19, identification of COVID-19 and vaccine progress through various symptoms" [3]. It is widely used to track the epidemic situation of COVID-19 worldwide. However, these systems were invented and were implemented separately. Thus, the connections bond between each part are really low. According to Nabil and Chakraborty, "It is difficult for managers to obtain uniform data on transmission, vaccination and detection. In addition, trust in testing data and vaccination data is problematic, especially in developing countries" [4]. Once the production quality of vaccine cannot be guaranteed, the results will be devastating. In addition, in the case of limited vaccine supply, if there is no systematic and standardized statistics on the data of a large number of vaccine candidates in the vaccination process, it is likely to cause confusion [5].

Blockchain is an innovation that focus on the distributed ledger technology, which can solve the problems of the currently popular area [6]. The blockchain, for instance, can help connect several different parts into one system, in which case they interact simultaneously without interfering with each other. All users will be a part of the maintenance of the system. If there is any change within the system, the system will automatically update. It provides transparent and clear data for all users, which has made great contributions to the establishment of Internet trust. It can also prevent any possible error, because all the data to be entered into the system will be received and screened by all

users. If more than half of the users in the system approve the data, the data can be successfully entered. At the same time, if someone intentionally provides any wrong input, it can be detected because it is a transparent system. Therefore, with the blockchain system, in the process of recording data, malicious damage to the system can be easily identified and held accountable [7].

2. Blockchain Technology and Architecture

2.1 Blockchain Technology Principles

2.1.1 Blockchain Builds Internet Trust

The concept of internet trust has arisen as a result of the rapid development of internet technology, which has greatly increased the number of its users and generated massive amounts of information [8]. Internet trust, which focuses on ensuring the authenticity and security of Internet information, has been successfully established by blockchain through technologies such as distributed networks, consensus algorithms, asymmetric cryptographic mechanisms and smart contracts.

2.1.2 Centralization and Decentralization

Decentralization is one of the key features of blockchain, but before that, people often used centralized systems [9]. The concept of centralization is similar to a large central database that stores information of all users. Centralization allows operations to be carried out without multiple judgements, saving time and increasing efficiency, but it also increases the risk of information leakage, for example if the owner of the central database has access to other users' information, or if the central database is attacked, all users' information is exposed to the attack.

Therefore, to ensure internet trust, blockchain uses the decentralization. In contrast to centralization which has a central database, decentralization constructs a large number of equal distributed databases to store data, through which every correct piece of information is stored in all databases at the same time, so it is difficult to tamper with the data in them.In blockchain, decentralization is just that, by storing data decentralized among a large number of nodes, where there is no overriding central node, but each node has equal rights and can all be regarded as a central node. As the number of nodes increases, the security of the blockchain rises, as does the cost of running the blockchain.

2.1.3 Consensus Mechanism

In order to guarantee the consistency of data in each node in a distributed network, the blockchain uses a consensus mechanism [10]. The origin of this mechanism is the "Byzantine failures". The "Byzantine failures" refers to a situation where multiple countries want to attack Byzantium, but because Byzantium is so powerful, the attackers cannot do it alone, instead attacking alone would lead to their own weakness and thus be attacked by others. However, a direct agreement between the attackers is also not guaranteed and there is no way to be sure that the other attackers will not betray and thus cause the attack to fail. And in the blockchain, to establish the authenticity of a message, it is also necessary to guarantee that more than 51% of all users approve it.

For this reason, blockchain has proposed a variety of consensus algorithms, mainly divided into two, one is BFT for solving the consensus problem in the presence of the Byzantine failures problem, and the other is CFT for solving the case where there is no Byzantine failures problem [11]. One of them, BFT, contains the famous POW and POS algorithms, POW means proof of work, an algorithm for assigning bookkeeping rights based on a hash problem that requires users to guess the corresponding value, a step that guarantees complete decentralization and great difficulty in cracking, but takes longer to reach consensus, the main user is Bitcoin. POS means proof of stake, the algorithm allocates bookkeeping rights by comparing the equity owned by users, shortening the consensus time, but as the equity owned by a single user increase, so does the likelihood that a user can complete an attack, the main user is Ether. These algorithms ensure that each node will comply with the agreement on its own, guaranteeing the best interests of the user.

2.1.4 Asymmetric Encryption

Blockchain uses asymmetric encryption methods to secure information when it is transmitted. Before asymmetric encryption, the usual encryption method used was symmetric encryption, which means that the same set of methods is used for encryption and decoding. In this method, once the secret key is broken, the message can be easily decoded by an attacker. Asymmetric encryption, on the other hand, uses two sets of keys, one for encryption and one for decryption, which greatly increases security. A well-known and widely used asymmetric encryption algorithm is the RSA algorithm, which first encrypts the message with the recipient's public key to avoid exposing the useful information directly in transmission, and then sends the encrypted message to the recipient, who then uses the private key to complete the decoding of the message. The public key is publicly visible and the private key is privately stored [12]. The details of the algorithm are as follows.

- First generate a set of public key private keys, choose two different prime numbers p, q, compute $N = p * q$, choose another prime number K at random, and compute D such that $K * D$ mod $(p-1)(q-1) = 1$, where (N, K) becomes the public key and D becomes the private key.
- Encrypt the message using the public key (N, E) to obtain $C = M\hat{}E$ (mod N).
- Decrypt the message using the private key (D) to obtain $M = C\hat{}D$ (mod N).
- There are many other mechanisms to use and extend the algorithms in practical applications of blockchain, including PKI to manage key generation, IBC to identify users and zero-knowledge proof to ensure information privacy.

2.2 Pros and Cons of Blockchain Technology

The two main advantages of blockchain technology are that it establishes internet trust and increases the security of information.

- Established internet trust: Blockchain technology builds a decentralized network through a distributed network and consensus algorithms. In this environment, everyone's nodes are equal and the algorithms ensure that each node will work to ensure the best interests of the user and the user does not have to worry about betrayal in the protocol, helping to build trust between the different entities in the network.
- Increased information security: Blockchain ensures that useful information is not exposed in the transmission path through asymmetric encryption algorithms, which makes it impossible for attackers to eavesdrop, greatly increasing the security of the information transmission process. Also, through the distributed network and consensus algorithm, the data is stored in multiple nodes, so an attacker cannot tamper with the information by attacking a single node, thus greatly increasing the security of information storage.

At the same time, as the use of blockchain grows, problems with blockchain are becoming apparent.

- The distributed network results in users losing their secret keys and then never being able to retrieve them.
- The POW algorithm used by Bitcoin requires a lot of computing power and can result in a lot of wasted energy.
- Consensus algorithms are at greater risk, such as the POS algorithm used by Ethereum. As the rights held by a single user become progressively larger, the greater the likelihood of a successful attack by that user, of which the Lido platform currently holds around 31% of pledged Ethereum, already approaching the baseline of 34%, which could pose a security risk in the future.

3. The Application of Blockchain Technology for COVID-19

3.1 Data Tracing for Medical Supplies

Mask plays an important role during the COVID-19 pandemic. At the begging of the epidemic in China, the demand for masks exceeded the supply. This phenomenon caused some merchants to sell

fake masks and many consumers suffered serious economic losses. Like mask, many other medical supplies are also faced with counterfeiting. Consequently, there is an urgent need for people to guarantee the medical supplies they received are effective. Blockchain has traceable characteristic. Every information is stored in a secure and tamper-resistant manner in the blockchain. Therefore, every data about medical supplies can be recorded in one blockchain system, and the traceability of blockchain can ensure these medical supplies are real and effective. At the same time, government can use this tracing system to supervise medical supplies to prevent illegal reselling, protecting consumer rights.

3.2 Reducing Logistics Cost

Lockdown is one efficient method to contain COVID-19. But huge logistics costs will cause great pressure on finance of a lockdown city which needs to contain epidemic at the same time and information opacity is one of the main reasons for the huge logistics costs. Transparency is an important feature of blockchain technology. With the support of blockchain technology, information about each link in logistics can be accessed in one platform, suppliers can provide materials more efficiently. Recipient can also get the information about logistics status in real time and trace the whole process of the production and transportation of supplies according to the traceability in blockchain.

3.3 Information Storage

It is inevitable that government need to collect vast quantities of information during the period of COVID-19 and such date contains a lot of personal information. But if the government has poor supervision or the database is vulnerable, which can easily lead to data leakage. Not only the property of people but also the life safety will be threatened. Decentralization is one very important feature of blockchain, which means every one could have their own database or node, users could access their personal information only use their own the private key. In other words, people can hold their information in their own hands without government or companies. Moreover, blockchain is a distributed database, every data calling in blockchain requires user authorization. This feature solves the problem of the data being abused by third party.

3.4 Track Supervision

According to the tracks of COVID-19 to find potential infected patients is an essential work during the epidemic. This task requires the precise time and place of the track of the infected patients. But if these is a large population carried virus and the range of the place they traveled is wide, track supervision will cost a lot of manpower and material resources. Using blockchain technology can help government to solve this problem more easily. Each place can generate a block in the blockchain network. The personal information of people who went through the place will add to the corresponding block. Aided by this blockchain system, manager can get the information about the number of people who passing the epidemic area and their time sequence easily.

3.5 Challenges

The security of blockchain technology is guaranteed by many encryption algorithms such as secure hash algorithm, symmetric encryption algorithm and asymmetric encryption algorithm. It is almost impossible for traditional computer to decrypted the messages encrypted by these algorithms. Because in terms of current computer performance, decoding the ciphertext requires thousands of years. Nevertheless, quantum computers, which use the phenomena of quantum machines, may decode some algorithms in a very short time, like RSA encryption based on integer factorization. Therefore, when quantum computers appear, blockchain requires to improve its encryption technologies to prevent the decline of safety.

4. Conclusion

The epidemic has occurred for three years. Blockchain technology is a key factor in preventing and controlling the epidemic and establishing Internet trust in preventing and controlling the epidemic. Through the investigation in Section 2, the characteristics held by the blockchain, namely decentralization and consensus mechanism, are powerful elements to enhance Internet trust. At the same time, the cryptographic encryption principle of blockchain is extremely secure before quantum computers and computers with stronger computing power are developed. After the discussion in Secion3, during the epidemic, blockchain technology will provide the following extremely useful points:

- According to transparent and clear data records, the addition of blockchain technology will strengthen the data records for the receipt and distribution of medical supplies.
- Through transparent processing of relevant information, blockchain technology can greatly reduce the logistics expenses during the closed epidemic period.
- Blockchain technology makes it possible to safely store personal information during the epidemic, rather than entrusting it to a third-party platform that cannot be completely supervised.
- Blockchain technology makes it easier to track people infected or spreading viruses maliciously.

References

[1] Hasan M R, Deng S, Sultana N, et al. The applicability of blockchain technology in healthcare contexts to contain COVID-19 challenges[J]. Library Hi Tech, 2021, 39(3): 814-833.

[2] Fusco A, Dicuonzo G, Dell'Atti V, et al. Blockchain in healthcare: Insights on COVID-19[J]. International Journal of Environmental Research and Public Health, 2020, 17(19): 7167.

[3] Nabil S S, Pran M S A, Al Haque A A, et al. Blockchain-based covid vaccination registration and monitoring[J]. Blockchain: Research and Applications, 2022: 100092.

[4] Gordon A, Reingold A. The burden of influenza: a complex problem[J]. Current epidemiology reports, 2018, 5(1): 1-9.

[5] Bettis A A, L'Azou Jackson M, Yoon I K, et al. The global epidemiology of chikungunya from 1999 to 2020: A systematic literature review to inform the development and introduction of vaccines[J]. PLoS neglected tropical diseases, 2022, 16(1): e0010069.

[6] Zheng Z, Xie S, Dai H N, et al. Blockchain challenges and opportunities: A survey[J]. International journal of web and grid services, 2018, 14(4): 352-375.

[7] Zhu X, Xu H, Zhao Z, et al. An Environmental Intrusion Detection Technology Based on WiFi[J]. Wireless Personal Communications, 2021, 119(2): 1425-1436.

[8] DiMaggio P, Hargittai E, Neuman W R, et al. Social implications of the Internet[J]. Annual review of sociology, 2001: 307-336.

[9] El Faqir Y, Arroyo J, Hassan S. An overview of decentralized autonomous organizations on the blockchain [C]//Proceedings of the 16th international symposium on open collaboration. 2020: 1-8.

[10] Wang Y, Cai S, Lin C, et al. Study of blockchain's consensus mechanism based on credit[J]. IEEE Access, 2019, 7: 10224-10231.

[11] Mingxiao D, Xiaofeng M, Zhe Z, et al. A review on consensus algorithm of blockchain[C]//2017 IEEE international conference on systems, man, and cybernetics (SMC). IEEE, 2017: 2567-2572.

[12] Lu Y. The blockchain: State-of-the-art and research challenges[J]. Journal of Industrial Information Integration, 2019, 15: 80-90.