Permissioned Blockchain: Leveraging Controlled Access for Diverse Sectorial Applications

Run Yan

School of Computing, Engineering & Physical Sciences, University of the West of Scotland
Lanarkshire Campus, Scotland, G72 0LH, United Kingdom
1807050102@stu.hrbust.edu.cn

Abstract. As technology advances, both institutions and individuals are increasingly prioritizing information security. Consequently, many enterprises and institutions are turning to distributed technologies that offer enhanced security for data storage and sharing, with blockchain technology emerging as a critical solution. This paper discusses the application of permissioned blockchain technology across various industries and compares its attributes with those of permissionless blockchains. The research indicates that permissioned blockchains provide distinct advantages in numerous sectors. Unlike typical blockchains, permissioned blockchains enhance data security and privacy through stringent access controls and authorization mechanisms. Furthermore, permissioned blockchains facilitate accurate authentication processes, reduce operational costs for enterprises and institutions, enable resource sharing, and provide robust protections against information theft. However, this paper also highlights some limitations in the current development of permissioned blockchains, including constraints on scalability, challenges in maintaining information trustworthiness, and impacts on decentralization. These issues require careful consideration as the technology continues to evolve.

Keywords: Permissioned Blockchain, Permissionless Blockchain, Application, Industries.

1 Introduction

Blockchain technology is currently regarded as one of the most transformative technologies. It operates as a decentralized and distributed data structure, setting it apart from traditional databases, which are typically centralized and managed by a single organization. Blockchain's development was initially spurred by the creation of Bitcoin by an individual known as Satoshi Nakamoto, serving as the foundational technology behind it. Modern systems highlight blockchain's unique attributes—transparency, provenance, fault tolerance, and authenticity—to support a range of distributed applications [1]. Today, numerous companies and institutions are leveraging blockchain technology. This raises several pertinent questions: What industries are best suited for permissioned blockchains? What limitations do permissioned blockchains face? What role do permissioned blockchains play across

Y. Wang (ed.), *Proceedings of the 2024 2nd International Conference on Image, Algorithms and Artificial Intelligence (ICIAAI 2024)*, Advances in Computer Science Research 115,
https://doi.org/10.2991/978-94-6463-540-9_36

various sectors? Addressing these questions is crucial for understanding and exploring the application of permissioned blockchain in diverse industries.

1.1 Permissionless blockchain

Bitcoin, along with many other different cryptocurrencies, is a permissionless blockchain. On a permissionless blockchain, any user can join anonymously and become a validator to check all transaction data and transactions on the permissionless blockchain. In such a network, without the intervention of a central organization and the management of smart contracts, all participating nodes do not have to worry about whether their transactions are threatened or unfair operations will occur. Simply put, on such a relatively transparent and fair permissionless blockchain, everyone is a participant manager and supervisor of information.

Because of the unique characteristics of blockchain, it has attracted much attention and is gradually being used in many industries today. However, due to the unique nature of some industries, they have more privacy needs to be kept confidential, so permissionless blockchain is not used in some industries. For example, in special fields such as banking systems, medical care, and public security systems, these systems contain a lot of information that cannot be released to the public. At this point, the advantages of permissioned blockchain come into play.

1.2 Permissioned blockchain

Its design and operating principles are similar to traditional blockchains, but differ in terms of permission management. On a permissioned blockchain, there are usually some access restrictions, and not everyone can access the data on the chain. Before users can access, users usually need to provide their identity information to a central agency or administrator for verification. Only those authenticated users can access information on the blockchain. This step has important implications for companies or systems that have confidential information. These companies can use this method to avoid interference from malicious users and information leakage.

1.3 Smart contract

Since the blockchain is very different from the traditional centralized architecture, the data stored in the data block cannot be changed once it is uploaded to the chain. In order to ensure the accuracy of each piece of information, a consensus mechanism emerged as the times require. Through the consensus mechanism, this system can reward conscientious nodes who can create acceptable blocks, and at the same time, this system can also punish some malicious nodes by seizing funds. Therefore, this mechanism can avoid the large number of malicious nodes from destroying the information authenticity of the blockchain. In permissionless blockchains, Proof of Work (PoW) and Proof of Stake (PoS) are commonly used. In the PoW mechanism, anyone can become a miner. By performing a large amount of calculations, they get the opportunity to upload their own packaged blocks to the chain, thereby obtaining cryptocurrency. In PoS, there is a certain threshold to become a miner, and the success of mining depends on the amount of cryptocurrency held. Among these participants, whoever holds the most tokens is most likely to become a miner. And if a validator behaves dishonestly or lazily during the verification process, the tokens they invested will be deducted. In permissioned blockchains, nodes establish consensus through an asynchronous fault-tolerant protocol (such as Paxos or PBFT) to determine the unique order in which transactions are appended to the blockchain ledger[2]. For PBFT, it means that in a distributed system, as long as the minimum percentage of nodes required behave honestly and function normally, then no matter what errors occur in other nodes (downtime, tampering, replay, etc.), the security of the network can be guaranteed.

2 Applications of Permissioned Blockchain in Various Sectors

2.1 Application in Identity Verification

Problems faced by identity verification today. With the current economic development and the increasing emphasis on humanistic care, governments of various countries are providing some special care and providing some benefits to special groups such as children, the elderly, and the disabled. The application and receipt of these benefits are usually linked to identity verification. In the past, these groups would have had their credentials verified to gain privileges. However, for this measure, fake certificates and fake privilege passes are becoming popular [3]. In addition, they can also obtain privilege cards through the official platform, but this method often consumes a lot of time and requires a large number of staff to handle online and offline processing for them. The wages of this group of employees are also a huge expense for the government. At present, the role of blockchain and Ethereum in smart contracts can be used to alleviate this problem.

Model design Apply. Applicants can apply for privilege cards through online platforms and offline service stations. They need to fill in some information, including their identity card number, disability certificate, etc. Once this data is filled in, it is automatically entered into the local database and the blockchain.

Verify: The prerequisite for being verified here is that the government has uploaded all the citizens' certificates to the blockchain and authorized them to relevant agencies for data verification. After matching the entered data with the data structure of the government system, its format and signature are checked [4].

Confirm: Information that has been verified is added to the blockchain, and the reliability of this information cannot be proven until the current blockchain containing this information is connected to the next blockchain. And once this information is added to the blockchain, it is difficult to change. In addition, all modifications to the information on the blockchain will be recorded one by one in the distributed ledger. As shown in Fig 1.

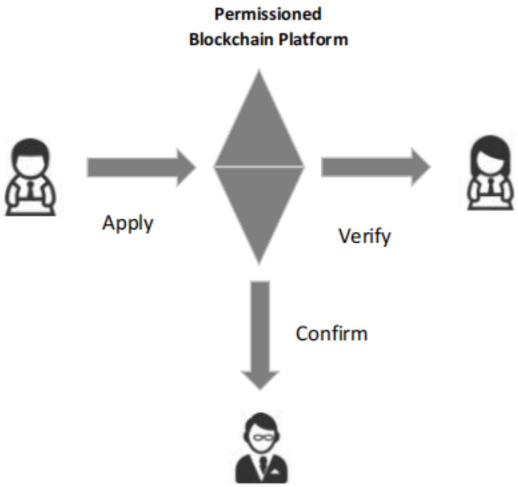

Fig.1. Permissioned Blockchain Platform.

In this system, the corresponding smart contract must be added to automatically issue privilege cards. When the applicant has completed all the required steps and has been successfully verified, the system can automatically issue the corresponding privilege card to the applicant.

2.2 Application in Healthcare

With the development of science and technology and the improvement of economic level, more and more people are beginning to pay attention to their own medical health. Many citizens conduct safety inspections regularly, and their requirements for compensation and liability determination for postoperative risks are becoming higher and higher. How to safely store patients' medical records, how to hold medical malpractice accountable, and how to quickly share patients' medical histories around the world have become a major challenge facing the current medical system. The Technology about blockchain is very useful in the medical industry. Currently, even if there are electronic files, doctors will transcribe the electronic files for archiving and preservation. Not only do these paper medical records take up a lot of space for storage in every hospital, but patients also need to pay corresponding fees when they want to download them. After investigation, it was found that the average cost of a copy downloaded from the Internet is 22 euros; a paper copy collected from the hospital costs 25 euros; and a paper copy sent by mail costs 28 euros [5].

These fees can be significantly reduced if blockchain technology is used. Doctors can store these medical records on the blockchain, and once the blocks containing this information are uploaded to the blockchain, they are difficult to change. And information security is also guaranteed. In addition to this, using permissioned blockchain also ensures the privacy of patient information. When a medical system uses permissioned blockchain, when doctors, nurses, or even individuals want to access patient information, the program will first verify their identities, and the system will automatically determine whether these visitors have permission to view the information. Therefore, patients can feel reassured about the confidentiality of their privacy. And through reasonable authorization, when patients encounter security threats around the world, doctors can view the patient's disease history through the data link, so that they can quickly provide correct first aid.

Faced with the issue of liability for medical malpractice, medical systems around the world are actively responding. The use of permissioned blockchain can reduce doctor-patient conflicts to a certain extent. During the patient's treatment process, the doctor's treatment measures and feedback will be recorded in the blockchain one by one and cannot be changed later. When a medical accident occurs, evidence collection personnel can conduct evidence collection analysis directly from the blockchain to determine liability. This can avoid the occurrence of contradictions such as unclear responsibilities and shirk of responsibility.

2.3 Application in Information Security

Problems faced by information security today. Information security is very important for both individuals and countries. If personal information is leaked, these people may be troubled by bank card theft, telecommunications fraud, etc. However, current passports and ID cards contain chips, but these chips pose certain information security risks. They are likely to be destroyed by criminals, leading to information leakage.

Modify or cancel information. At the beginning, users need to fill in the passport information from scratch. After completing the filling, the system will store the information in the blockchain, and the system will issue a unique ID to this information. When a user wants to modify the information due to personal circumstances, the system will not directly overwrite the original value with new content. Instead, issue an ID separately for this new piece of information. When a user wants to cancel his or her passport, the user only needs to provide the previous unique identifier to cancel. However, the logout here does not delete the original information in the blockchain. This information still exists in the database, but continues to create a new transaction ID. It's just that the user's personal status has been logged out in the blockchain.

View modification history. And a historical record registry is also created in this blockchain to record the specific information of each transaction. For example: trading time, executor who performed the transaction, etc. Because the historical registry system may query the historical registry using SQL, a conventional database, finding specific information using it may be faster [6].

Hierarchical management of the system. Since a large amount of private information of citizens is stored in this blockchain, this blockchain cannot be completely transparent, and all information stored on it cannot be viewed by all visitors. Here the system can classify visitors into different categories. And control the storage security of information by giving them different permissions. Visitors can be divided into two categories here: system administrators and users. In order to make management easier, they will group users and manage them by adjusting user permissions [7]. Under normal circumstances, these users can usually only access their own personal information and information related to themselves (children, spouses, parents, etc.).

Due to the unique nature of private chains, unrelated parties usually cannot see other people's information. At the same time, changing the value on the blockchain requires the support of 51% of the computing power [8]. Once the information is stored in the blockchain, it is difficult for hackers to tamper with and attack it. In this way, even if a hacker maliciously modifies the contents of the passport or ID card, the details of the modified information can be seen at a glance by viewing the historical record registry on the blockchain. The use of permissioned blockchain can not only combat the theft of information by hackers, but also help the police capture cybercriminals.

2.4 Application in information synchronization

The current problems faced by information synchronization. Information synchronization can increase work and learning efficiency, but there are still many jobs today that cannot achieve strong information synchronization. For example, in terms of article publishing, in order to publish academic results, scholars usually need to conduct a large number of tedious communications with editors and other collaborators in order to improve the article publishing process. However, these scholars and corresponding editors usually rely on some traditional communication media to follow up on the project, such as making phone calls, sending messages, sending emails, using specific websites, etc [9]. These traditional communication media make it difficult to follow up on information. And before the article is published, the article needs to be reviewed by reviewers to determine whether the article meets the publication standards. The entire review process is also a challenge for writers. They cannot check the reviewer's progress at any time and can only wait for a long time. If the results are unsatisfactory, it is difficult for the writer to know the detailed reasons and they can only submit a reconsideration to the organization. The whole process is time-consuming and inefficient. The introduction of blockchain technology into this field will have a profound impact on improving the transparency of the publishing process.

Use permissioned blockchain to solve the problem of out-of-sync information. Now, if permissioned blockchain technology is used, this problem can be solved very well. On the blockchain, the entire review process is open and transparent. Writers can check the reviewers' updates at any time, as well as their detailed suggestions and final results. This avoids disputes over the final result and increases publication efficiency. In addition, due to the particularity of permissioned blockchain technology, participants must be authorized through real-name verification to gain access.

Therefore, the relevant information of the author's article can be protected through permissioned blockchain technology.

2.5 Application in information tracking

Difficulties currently encountered. In many countries, in order to stabilize the price of special commodities and ensure their quality, the government will conduct macro-control on them, carry out fixed-point quantification, and planned manufacturing and processing. Cannabis has become a legal substance in Canada. In order to ensure the safety of cannabis, the government controls the production quantity and issues product approval labels to designated production plants. Only cannabis with an approved label is recognized by the Canadian government as legal cannabis. In addition, in order to regulate the government, these companies also need to provide import and sales data related to cannabis. These companies include hospitals, factories, etc. that produce medical cannabis. In order to accurately record these data, relevant companies usually hire a large number of professional teams to organize and maintain data, which will increase the company's operating costs and thus also increase the sales price of cannabis. Once the cost increases, users will often choose black market products with lower prices, so it will be difficult for these officially produced cannabis to attract those users. And some workers will illegally trade the licensed labels to obtain profits. How to quickly verify the authenticity of the label and the source of production has become a difficult problem in current cannabis supervision.

Monitoring and management using permissioned blockchains. In a permissioned blockchain, governments can often connect these tags with producer or factory metadata. Through this method, the real-time status of cannabis in the supply chain can be quickly queried, thereby reducing illegal transactions of labels. And even if criminals do something illegal, they can still find it out through the distributed ledger.

3 Challenges in the Development of Permissioned Blockchain

3.1 Scalability

Today, many businesses and institutions depend on permissioned blockchain technology, yet they face significant challenges related to scalability. In numerous applications, the scalability constraints of permissioned blockchains hinder their ability to process multiple transactions simultaneously, which slows down response times and degrades user experience. However, this scalability issue can be addressed using Apache Spark's MLLib [10]. The core principle of Apache Spark involves enhancing the speed of operations across memory clusters, which enables it to manage information parallelism effectively. In the blockchain architecture, which comprises four layers, Spark's role is pivotal at the application and consensus layers. It processes transaction requests and routes them to the Kafka cluster. Within this cluster, transactions are subjected to a random forest algorithm, which facilitates their sorting and parallel processing. This technique significantly enhances the scalability of the blockchain, ensuring that even with up to 30,000 transactions, the confirmation time remains nearly consistent. This advancement not only optimizes transaction handling but also ensures that blockchain systems can scale efficiently to meet growing demands. As shown in Fig 2.

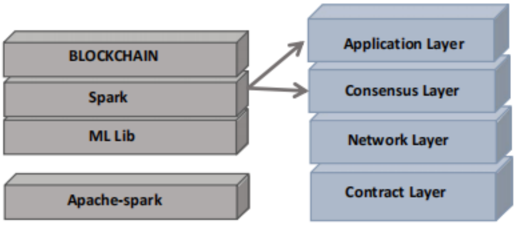

Fig. 2. Optimization solutions for scalability .

3.2 Trustworthiness of Information

There is a difference between Permissioned blockchain and permissionless blockchain. In a permissionless blockchain, everyone can participate in the verification process of transactions in the blockchain anonymously and have the opportunity to become a verifier. However, since the permissioned blockchain has certain permissions, only the central manager can manage it. If the central manager tamperes with the data, the credibility of the information existing in the data chain will be greatly reduced.

3.3 Risks to Decentralization

If authoritative and privileged nodes get out of hand, or if consensus cannot be reached, the network will collapse. Because permissioned blockchains are not completely decentralized, many of the features and advantages of blockchains will be lost, making it difficult to ensure the security and authenticity of data.

4 Conclusion

This article examines the characteristics of permissionless blockchains and conducts a comparative analysis with permissioned blockchains. Permissioned blockchains are found to be better suited for applications demanding high security and privacy levels, such as medical records containing sensitive personal information, government databases securing national security details, and other similar institutional uses. On the other hand, due to their high degree of decentralization and transparency, permissionless blockchains are more apt for projects requiring extensive public oversight, such as donations and crowdfunding initiatives. Despite the increasing maturity of permissioned blockchain technology, future challenges such as scalability, information transparency, and corruption risks remain critical issues that need to be addressed.

References

1. M. J. Amiri, D. Agrawal, & A. El Abbadi, Permissioned blockchains: Properties, techniques and applications, In Proceedings of the 2021 International Conference on Management of Data (2021), pp. 2813-2820.
2. H. S. Lamkuche & S. Prasad, Smart Contract-Based Free Privilege-Pass Authentication System for Indian Railway Using Permissioned Blockchain.
3. G. Capece & F. Lorenzi, Blockchain and Healthcare: Opportunities and Prospects for the EHR, Sustainability, 12(22) (2020), 9693.
4. N. Jahan, S. Reno, & M. Ahmed, Securing E-passport management using private-permissioned blockchain and IPFS, In 2023 International Conference on Electrical, Computer and Communication Engineering (ECCE) (2023), pp. 1-7.
5. X. Zhu, H. Xu, Z. Zhao, & others, An Environmental Intrusion Detection Technology Based on WiFi, Wireless Personal Communications, 119(2) (2021), 1425-1436.
6. S. Solat, P. Calvez, & F. Naït-Abdesselam, Permissioned vs. Permissionless Blockchain: How and Why There Is Only One Right Choice, J. Softw., 16(3) (2021), 95-106.
7. Y. Bao, Z. Gui, Z. Sun, Z. An, & Z. Huang, Spatial Blockchain: Enhancing Spatial Queries and Applications through Integrating Blockchain and Spatial Database Technologies, Electronics, 12(20) (2023), 4287.
8. M. Kouhizadeh, Q. Zhu, & J. Sarkis, Blockchain and the circular economy: potential tensions and critical reflections from practice, Production Planning & Control, 31(11-12) (2020), 950-966.
9. A. Ali, H. A. Rahim, M. F. Pasha, R. Dowsley, M. Masud, J. Ali, & M. Baz, Security, privacy, and reliability in digital healthcare systems using blockchain, Electronics, 10(16) (2021), 2034.
10. J. Duchenne, Blockchain and smart contracts: Complementing climate finance, legislative frameworks, and renewable energy projects, In Transforming climate finance and green investment with blockchains (2018), pp. 303-317.