Blockchain Technology in Metaverse and Its Safety Problem

Yifan Yin[1,*], Hongkun Yang[2], Zicheng Shan[3]

[1]Department of Mathematics, University of Illinois at Urbana-Champaign, Urbana-Champaign, 61801, USA
[2]Department of Mathematics, New York University, New York City, 11201, USA
[3]Department of Computer Science, University of Utah, Salt Lake City, 84112, USA

yifany10@illinois.edu, hy2363@nyu.edu, u1445545@umail.utah.edu

Abstract. At present, the digital economy produces a large amount of data, which can be protected by using the irreversible and unmodifiable characteristics of blockchain to solve the protection requirements of non-physical forms and within reach. Thus, the link between virtual assets and reality can be effectively protected. This article covers blockchain operation, and introduces the concept of the universe and potential application scenarios. Also, it covers requirements of computer blockchain facing problems, and the way to make full use of resources in a limited work force and save resources. In order to achieve the best condition and be more friendly to the environment of resource utilization, therefore, puts forward the work force allocation.

Keywords: Metaverse, blockchain, safety problem, application

1 Introduction

1.1 Metaverse

The metaverse refers to a virtual world that is completely separated from the physical world, where people in real life have a cyber doppelganger. Its realization in today's world will be supported by the computer as the key underlying technology, and it will virtualize the living environment of every user, not only limited to a certain user but the living environment of the whole human being.

1.2 Blockchain

What is Blockchain? According to Ludovico, a blockchain is a data structure that contains a list of blocks. These blocks store different important data and information. To be more specific, there are several elements in each block. Firstly, the block contains the transactions that the miners decide [1]. Secondly, the block will contain the hash value from the last block. This information connects each block and becomes a chain.

A. Holl et al. (Eds.): ICHESS 2022, ASSEHR 720, pp. 2114–2120, 2022.
https://doi.org/10.2991/978-2-494069-89-3_242

Thirdly, each block contains a timestamp, and each timestamp is unique for each block. More importantly, a block is verified to be valid "only when its timestamp is greater than the median timestamp of the previous 11 blocks" [1]. Fourth, each block owns a random number called the nonce. The nonce is useful in determining the next block. Before adding to the blockchain, each block is supposed to be hashed through the SHA-256 cryptographic function. The result of the hash of the block must be in a specific range, difficulty target which is determined by the zeros that the hash value starts with. Thus, the difficulty target can be "dynamically adjusted" depending on the computing power of the system. When the power is strong enough, the target narrows. For example, when more powerful machines add to the system, the target will narrow. If the computing power of the system is low, the difficulty target will broaden. By doing so, a new block will be mine every 10 minutes on average.

Application of Blockchain. Blockchain technologies can provide freedom to edit the software code, access, read, and change the content of the Blockchain, and participate in the consensus process. A public Blockchain mostly builds on open-source code; anyone can access the Blockchain, provide modifications, and contribute to the consensus process. Since blockchain can be used in decentralized operation and verification, it is possible to be used in the voting system [2]. Blockchain can keep the voter opinions in each block which prevents the voter to vote repetitively. More importantly, the data stored in the blockchain is impossible to be changed; thus, the voting result must be completely fair. Moreover, the blockchain is now widely used in the field of finance such as banking and stock trading [2]. Therefore, it is possible that people can change their real money to some data on the blockchain.

2 Why is Metaverse Important?

Within the virtual world, it is easy for users to try different things they cannot do or will not choose to do. For the experimenters, they can conduct an experiment, collect results from the computers, and store the data in a digital form with extremely low environmental cost. Moreover, it is possible to withdraw the digital experiment, but it is not possible to do that in the real world. Thus, experiments such as nuclear related ones may be conducted easily and securely in the metaverse [3].

One important application of metaverse is related to the major software technology breakthrough in AI today: autonomous driving. The program is artificial intelligence, which requires a lot of data to be adjusted and gradually stabilized. The only way to obtain data today is to drive the cars on the road. This way has great potential risks and uncertainties such as car accidents. Moreover, it also requires the participation of experimenters and the payment for them will be costly. If the company choose to put the experiments in metaverse, where it is completely digitized and controlled by computers, it may be significantly less costly than in the real world, and the data available will be more diverse. Users can also choose to add various possible and potential emergent cases in order to train the algorithm, which will be more conducive to the optimization and improvement of artificial intelligence. Because its underlying support platform is computer, which has the characteristics of continuity, stability, real-time data pro-

cessing ability and so on, it can greatly save costs for relevant enterprises and effectively control unexpected risks from the economic aspect, and data mining in it will be more thorough and comprehensive. In addition, the most significant advantage for avoiding downtime due to special accidents can achieve real 7 by 24 hours non-stop training, and can choose to configure better computer hardware through the time level and does not reduce the project as the basis, accelerate the training process greatly shorten the training cycle has incomparable advantages with the reality.

3 Function of Blockchain

3.1 About Data Trading

Zhang indicates that blockchain system allows the users to have a private and high-secure data trading process [4]. According to Zhang's model, the data supplier will upload subscripts and indexes to the data trading system as the first step. If there are data demanders that apply for the data from the trading system, the trading system requires the demanders to upload the algorithm that needs the data and the corresponding hash value [4]. Then, the data trading system will generate a pair of public keys and private keys and send the public key to the data supplier and the data demander. Next, the data supplier will encrypt the data with the public key and upload the encrypted data to the data trading system. After that, the trading system will decrypt the message from the supplier and use the algorithm provided by the data supplier to calculate the result that the data demanders need in the beginning. Next, the trading system will encrypt the calculated result with the demander's public key and send the message to the demander. Finally, the system will destroy the information in the system for this transaction such as the algorithm and the data. This trading system can provide the users a safe transaction environment online [4]. Since the data will not be stored neither by the system nor by the data demander, the data will not be compromised, and this system secures the intellectual property of the data supplier.

Take advantage of the optional decentralization of blockchain to store data access, transaction and usage records, avoiding unilateral non-recognition or breach of contract. When faced with complex businesses that cannot be handled online such as some businesses that require cash checks, the advantages of blockchain can be used to record simple information and correspond with real business (or objects). Storing the information in the block or in the metaverse, it is secure for the users to get accurate information for offline activities such as the trading amount and trading prices.

Applying this trading system in the metaverse, each user can safely trade its data to other users and help other users to get the information they truly need. For instance, it allows users to train AI in the metaverse with the support of this trading system. Since neither the system nor the data demander knows the main data, it not only helps the data supplier to secure the data, but also assists the demanders in training the AI. There are other cases that can use this trading system to secure the privacy of the data.

However, there are some situations where this algorithm is not working. In some cases, the data demanders require the actual data instead of just the result out of the algorithm. For instance, if users want to listen to music, they require the platform in the

metaverse to provide actual music to them. Thus, it is possible for these users to record the music and send the record in the metaverse which will form music piracy. Therefore, to protect the intellectual property of the users in the metaverse, there should be some technical developments.

3.2 About Privacy

Wang provides a new method that can secure multi-party auditable blockchain signature schemes and design a credible evaluation mechanism for the participants. The mechanism is composed of a trust vector with timestamps and a trust matrix with multi-dimensional vector groups [5]. If the participant passes the evaluation mechanism and is considered to be credible, a secure and trusted signature scheme is constructed through a secret sharing technology. This scheme can effectively reduce the damage caused by malicious participants. Implementing this method in the metaverse can solve many privacy issues. By evaluating the participants' credibility, the malicious participants' activities including stealing information will lead to decreasing credibility in the metaverse. When the credibility is below the restricted level, these malicious participants' activities in the metaverse will be limited. Therefore, the environment of the metaverse should be more secure. Moreover, Wang introduces a system to calculate the credibility points which can be useful in the trading system as well. The credibility system will evaluate the user's credibility based on their daily activities [5]. For each transaction in the trading system, the metaverse will require the demander to provide their own credibility point. Meanwhile, the system will ask for the lowest credibility point that the suppliers accept. The transaction will proceed only when the credibility point of the user is higher than the limit of the supplier. With the limitation on the credibility, the trading environment will be secure.

3.3 About Supply Chain

According to Xu, Electric-based Supply Chain (ESC) model is a method to deal with the difficulties between the consensus mechanism of the blockchain and the support for goods supply chain anatomy. In the ESC model, the credit score of a node was first calculated according to the smart contract activities by this node. Then, from the perspective of game theory, the influences of node active degree and credit score on stake under ESC were analyzed [6]. Finally, Xu provides experiment results to prove the method is effective. With the support of the ESC, the traditional target of public disclosure is divided into nodes, which is convenient to save resources and improve the use efficiency of resources [6]. Moreover, ESC Introduces smart contracts to automatically record the interaction between the two parties, avoid subsequent disputes and improve communication efficiency, etc., and synchronize the contracts to the blockchain [6]. When applying this ESC model in the metaverse, the economic system in this digital world can work as effectively as the one in the real world. Moreover, with the support of the blockchain and smart contracts, the transaction details can be protected, which makes the transactions in the metaverse even more secure than the ones in the real world.

4 Safety Problems

Metaverse is still a concept in development, there are still a lot of difficulties that need to be resolved. Blockchain is one of the most important base techniques for building a metaverse. Though this technique is already well-developed compared to others such as brain-machine interface, there are still problems with it. Blockchain served as a trading system in metaverse. As a trading system, the most important thing is safety. However, in the past few years, there have been several successful attacks on blockchains. Though most of the attacks can be defended by improving the codes and algorithms, there are still attacks that need specific ways to defend them. Here are two examples.

4.1 Finney Attack

Finney attack is a double spend attack based on block declaring time aimed at traders that accept 0-confirmation trade. The attacker first starts transaction 1 that transfers all digital cryptocurrencies in location A to location B. Then joins mining. The attacker will eventually arrive at block 1 which records transaction 1. Then the attacker keeps that block undeclared and starts another transaction 2 using digital cryptocurrencies in location A with a trade accepting 0-confirmation trades. After block 2 which records transaction 2 and the attacker receives the goods, the attacker declares block 1. Since transaction 1 happens before transaction 2, the system will find there are not enough digital cryptocurrencies in location 1 for transaction 2 and make transaction 2 invalids. In this way, the attack succeeds. According to Wei, the way to defend the Finney attack is to refuse all 0-confirmation trades because under PoW consensus, usually waiting for 6 confirmations can prevent the transaction from becoming invalid on the longest chain [7]. This can be easy at present, but when in the metaverse, much more traders will join than now and not all traders want or even have the time to wait for conformations. So other solutions are still needed.

4.2 51% Attack

When the attacker has more than half of the hashrate of the blockchain, the attack becomes easy. After the attacker finishes a transaction. All he needs to do is to start mining on a side chain generated on a fork before the block contains this transaction. With more hashrate than all other miners, soon he can make the side chain longer than the main chain and become the new main chain. Then his trade will become invalid, and the attack succeeds. “The only way to defend is to make the hashrate distribution more decentralized and there is no way to resolve this on technical level based on PoW consensus.” [7]. In another word, this still cannot prevent 51% attack from happening. “While developing bitcoin, Satoshi Nakamoto tried to use economical principle to prevent 51% attack. Since the cost for gaining 51% hashrate is extremely high, and after the attack occurs because of crisis of confidence, the digital cryptocurrencies will seriously devalue. So, if someone gets that high hushrate, being a miner still gains more than becoming an attacker.” [7]. However, when it is in the metaverse where blockchain can be the base economic system, it is extremely dangerous if there is a way to devalue

a currency that fasts. Moreover, the attacker may not aim to gain money when he starts a 51% attack then the economical principle cannot protect traders anymore. Even if the attacker is aimed at money, there are still ways to lower the cost of 51% attack:

Bribe Attack. In a bribe attack, after attacker's transaction is completed. He promises to provide more rewards for those miners who work on the second longest chain. In this way, he can attract other miners to work on that chain and gain 51% hashrate to make the longest side chain become longer than main chain and make it the main chain.

Coin Age Accumulation Attack. This attack method works on "PoW + Pos" based blockchain. In this kind of blockchain, one location has the more digital cryptocurrencies in hold and the longer time digital cryptocurrencies are on hold. This location has the easier difficulty to mine [7]. So easier to get to new block. In this way, it is easier to get 51% hashrate.

General mining attack. This way is used to attack those digital cryptocurrencies similar to mainstream digital cryptocurrencies but do not have a large mining scale yet, especially altcoin of mainstream digital cryptocurrencies [7]. In this kind of blockchain, 51% hashrate is much easier to be reached. Since the attack is aimed at money, so the attacker can sell all the digital cryptocurrencies gained immediately after getting them before the devaluing because of crisis of confidence.
According to the above, before blockchain technology is ready to be used to build metaverse. The safety problem must be resolved before applying to the metaverse.

5 Conclusion

This article discusses the potential applications of the blockchain systems in the future development of the metaverse. The blockchain can provide a secure trading environment including supplying and selling, and offer users private online spaces. However, there are still potential problems that may possibly interfere with the development of the metaverse which needs future technology to conquer.

6 Acknowledgement

Yifan Yin, Hongkun Yang, and Zicheng Shan contributed equally to this work and should be considered co-first authors.

7 References

1. Rella, Ludovico. "Blockchain." International Encyclopedia of Human Geography, edited by Audrey Kobayashi, Elsevier Science & Technology, 2nd edition, 2020. Credo Reference,

http://proxy.library.nyu.edu/login? url=https://search.credoreference.com/content/entry/esthuman/blockchain/0?institutionId=577. Accessed 23 Jun. 2022.
2. Henderson, Harry. "blockchain." Encyclopedia of Computer Science and Technology, Harry Henderson, Facts On File, 3rd edition, 2017. Credo Reference, http://proxy.library.nyu.edu/login? url=https://search.credoreference.com/content/entry/fofcomputer/blockchain/0?institutionId=577. Accessed 24 Jun. 2022.
3. Meng, Yonghui "Blockchain: A 'bridge' that combines virtual and real'", https://baijiahao.baidu.com/s?id=1717585074892961119&wfr=spider&for=pc.Accessed July 15, 2022
4. ZHANG Xuewang, YIN Zijie, FENG Jiaqi, YE Caijin, FU Kang. Data trading scheme based on blockchain and trusted computing[J]. Journal of Computer Applications, 2021, 41(4): 939-944. http://www.joca.cn/CN/Y2021/V41/I4/939. Accessed 1 July 2022
5. WANG Yunye, CHENG Yage, JIA Zhijuan, FU Junjun, YANG Yanyan, HE Yuchu, MA Wei. Auditable signature scheme for blockchain based on secure multi-party[J]. Journal of Computer Applications, 2020, 40(9): 2639-2645. http://www.joca.cn/CN/Y2020/V40/I9/2639. Accessed 1 July 2022
6. Xu Yuntao, Election-based supply chain： a supply chain autonomy framework based on blockchain[J]. Journal of Computer Applications, 2022, 42(6): 1770-1775.http://www.joca.cn/CN/Y2022/V42/I6/1770. Accessed 2 July 2022
7. Wei, SongJie Overview on Typical Security Problems in Public Blockchain Applications. Ruan Jian Xue Bao/Journal of Software, 2022, 33(1): 324–355 (in Chinese). http://www.jos.org.cn/1000-9825/6280.htm