


## Article

# Using Blockchain to Protect 3D Printing from Unauthorized Model Tampering

Yajing Wang, Yaodong Yang \* , Shuaipeng Suo, Mingyuan Wang and Weifeng Rao \*

School of Mechanical Engineering (Shandong Institute of Mechanical Design and Research), Qilu University of Technology (Shandong Academy of Sciences), Jinan 250353, China

\* Correspondence: yaodongy@qlu.edu.cn (Y.Y.); wfrao@qlu.edu.cn (W.R.)

**Abstract:** As three-dimensional (3D) printing technology is widely used, security issues have arisen, especially in the terminal parts of automobiles, aircraft, and 3D-printed military equipment. If the original design models or the STL (stereolithography) files are hacked or tampered, severe consequences can be anticipated. In this paper, we propose a demonstration to use a high-throughput blockchain to store the “fingerprints” of the 3D model and verify the “fingerprints” before printing to prevent illegal tampering. Relying on the tamper-resistant features of blockchain, the security of the model and the credibility of the terminal components can be ensured. The combination of blockchain and 3D printing will help people to build a trusted manufacturing environment and realize a more flexible manufacturing for future industry.

**Keywords:** STL file; copyright protection; blockchain; sharding; additive manufacturing



**Citation:** Wang, Y.; Yang, Y.; Suo, S.; Wang, M.; Rao, W. Using Blockchain to Protect 3D Printing from Unauthorized Model Tampering. *Appl. Sci.* **2022**, *12*, 7947. <https://doi.org/10.3390/app12157947>

Academic Editor: Richard (Chunhui) Yang

Received: 28 June 2022

Accepted: 3 August 2022

Published: 8 August 2022

**Publisher's Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



**Copyright:** © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

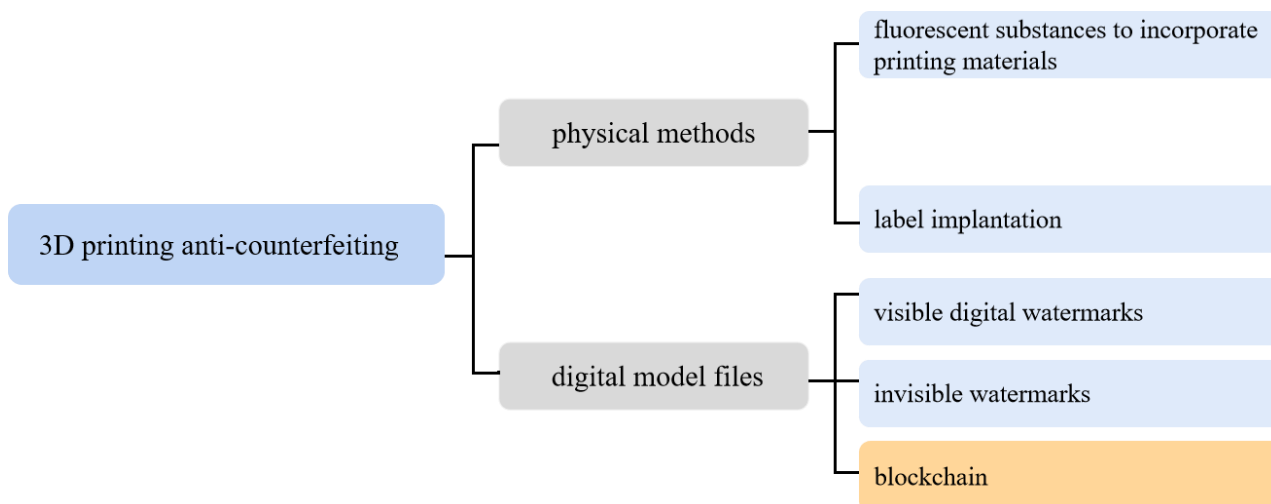
## 1. Introduction

To meet the increasingly diverse requirements in modern society, a part of traditional centralized large-scale manufacturing will transform into distributed flexible manufacturing that is characterized by highly customized and rapid production. Different from the traditional material processing techniques (e.g., removal, cutting, and drilling processing) [1], additive manufacturing (AM), also known as rapid manufacturing technology or 3D printing, fits this requirement. It starts from an STL (stereolithography) model design and then builds up a complete object layer by layer via printing [2]. It has become increasingly important in producing automobile parts, medical implants [3], unmanned aerial vehicles, and military equipment [4,5]. AM is bringing a new round of industrial revolution and its widespread proliferation may reform traditional manufacturing. For example, the 3D printing industry has grown exponentially and the market size was close to USD 12.8 billion in 2020 [6]. According to Google Scholar searching, research papers related to AM are increasing year by year, and the number of papers on AM exceeded 80,000 by the end of 2021.

However, with the rapid development of additive manufacturing, a heavy reliance on digital data makes people deeply concerned about the theft of intellectual property and other infringement acts. Since the advent of additive manufacturing, “additive manufacturing fraud” has been frequently heard about around the world. During the explosion of 3D printing (2011–2021), criminals were found to use 3D printing to create fake card slot password-stealing devices in various parts of Europe and the United States. It was found that counterfeiters used 3D printing technology to copy security seals and steal drugs in containers [7]. Recently, it was also reported that criminals have used 3D printers to mass-produce counterfeit products and caused huge losses to consumers and genuine manufacturers [8]. Loopholes in the 3D printing process can cause problems too. In 2017, Dr0wned demonstrated a representative 3D printing infringement experiment: the experimenter invaded the STL model and implanted a defect in the blades of a quad-rotor

UAV (unmanned aerial vehicle), causing it to fall in a short time [9]. The accidents caused by abusing additive manufacturing are far more than this. A large number of printed counterfeit products will not only lead to great harm to the original creators and designers but even endanger the entire additive manufacturing industry. How to effectively reduce counterfeit products and protect the intellectual property rights of STL model files become major problems in the current additive manufacturing industry.

Currently, there are two main ways to realize 3D printing anti-counterfeiting (Figure 1). One is by physical methods, including using fluorescent substances to incorporate printing materials [10–12], label implantation [13], etc. However, these methods all require special equipment for scanning/reading (e.g., X-rays or ultraviolet devices) and the verification process is cumbersome, time-consuming, and costly. Another anti-counterfeiting idea is focusing on model files. Digital watermarks can be embedded into the models directly [14], including 3D visible digital watermarks [15,16] and invisible watermarks [17,18]. However, 3D printers with different precisions will affect detection [19] and the detection process of these watermarks is also cumbersome. Generally, grid reconstruction or printing directions are required to obtain the printing direction according to print traces to see the watermarks [19]. In fact, the above anti-counterfeiting works mainly focus on protecting printed items. Due to the process of a product involving multiple segments, it is not enough to just protect the final step. The digital model files may also be forged quite easily. These methods are invalid once unauthorized model tampering happens. If the upstream has been an intrusion, it will be useless for the downstream to do more work. From the perspective of protecting the whole industrial chain, it is crucial to pay close attention to STL files at the beginning.



**Figure 1.** Types of 3D printing anti-counterfeiting methods.

To explore a better way to protect digital model files at the upstream, we propose to use blockchain technology to ensure STL model printing is authentic and credible from the source.

## 2. Design and Analysis

### 2.1. Choosing an Underlying Blockchain

As a new technology followed with great interest, blockchain was initially used as the underlying network of digital currency (a famous example is bitcoin, which is the flat currency of the Republic of El Salvador). Now, blockchain is also involved in many industries including copyright protection, traceability, medical treatment records, etc. People create trust and credible networks for supply chains based on blockchain technology, which can ensure the records are accurate and reliable. Blockchain provides a way for each member (or node) of the entire network to obtain all the records of transactions. In this

network, each member maintains its ledger and all the actions will be recorded. When new data are produced and stored, a block will be added to the previous block in a strict order. These blocks connect end to end and form a chain. Data on the chain can be transactions, assets, identity, or anything that can be described in digital form, and these records are permanent, transparent, and searchable. There are some reported blockchain-based 3D printing anti-counterfeiting works. Kurpjuweit et al. concluded that blockchain would improve additive manufacturing supply chains and act as a secure inter-organizational intellectual property management layer [20]. Alkhder et al. developed a blockchain-based 3D printing solution to track data from the supply process of 3D-printed products [21]. The above two works focus on the data service of the 3D-printed product supply process. We pay more attention to protecting the security of the model during internet transmission which is a fragile link prone to infringement.

When considering the blockchain industry, the first question is which blockchain to choose. In the manufacturing world, a very-high-throughput (characterized by transaction processing per second, TPS) blockchain is needed to meet the requirement of recording and processing a large amount of manufacturing data. Therefore, it is completely infeasible to use a bitcoin network to process manufacturing data since the TPS of a bitcoin is only 7 [22]. Ethereum was first proposed by Vitalik Buterin in 2013, aiming to become a global open source blockchain platform able to support diverse applications. However, the throughput of Ethereum is also very low, around 15 TPS [23]. To improve the throughput capacity of a blockchain, some potential strategies, such as increasing the block size [24], sharding [25], and developing a second layer (also called two-layer strategies) [26], have been discussed and developed. Among them, sharding technology is very suitable for manufacturing scenarios because it considers both the security and the high throughput [27]. After examining the major characteristics of existing mainstream sharded blockchains (see Table 1), it is believed that the QuarkChain [28] network is one of the most effective platforms to implement the protection of the STL model. Because QuarkChain consists of two layers, the first layer consists of many sharding chains (or sub-chains) for recording detailed transactions. The second layer is a master chain used to confirm transactions and ensure the safety of the sub-chains. The number of sub-chains can be dynamically increased, so the overall throughput of the network will improve according to the needs of manufacturing. In a testing environment, a sharding blockchain can reach tens of thousands or even hundreds of thousands of TPS [28]. Moreover, it supports Turing complete smart contracts and can also satisfy the automatic execution of our various instructions [28]. A structure diagram of the QuarkChain system is shown in Figure 2.

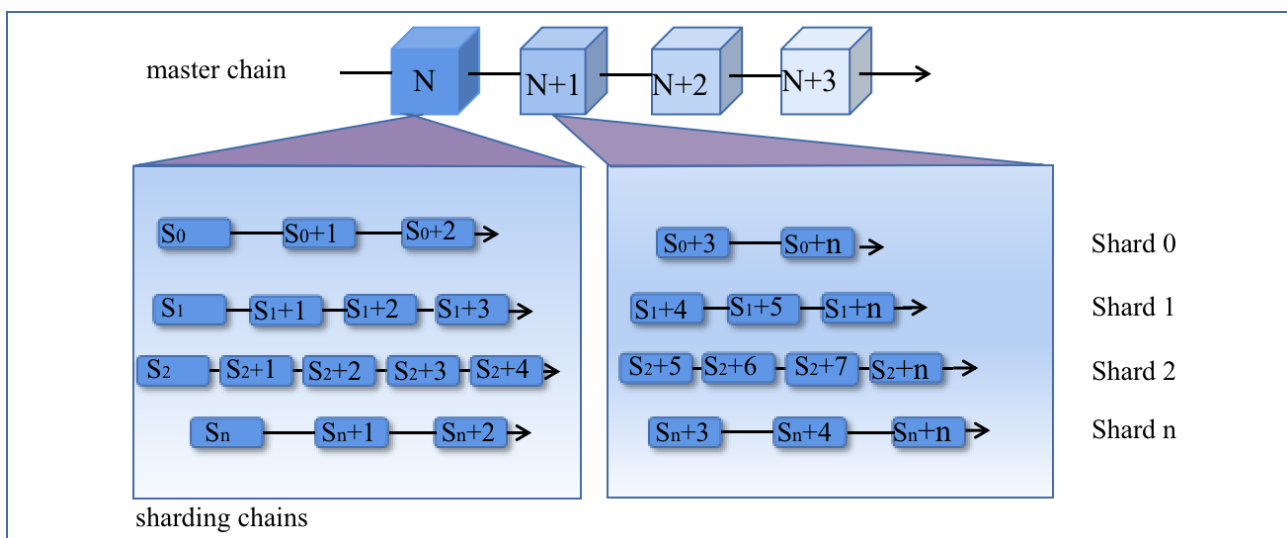


Figure 2. A high-throughput blockchain with a sharding framework.

**Table 1.** Comparison of several sharding blockchains.

Network	Transactions per Second	Characteristics	Types of Sharding
Zilliqa	2488 TPS	<ul style="list-style-type: none"> <li>Divided into multiple shards, each shard includes a committee and miners.</li> <li>The entire network has linear scalability.</li> </ul>	Network sharding*; transaction sharding**
QuarkChain	≥100,000 TPS	<ul style="list-style-type: none"> <li>Consists of a two-layer structure of root chain and fragmentation.</li> <li>Without affecting the root chain, the number of shards in the shard layer can be dynamically increased.</li> </ul>	Network sharding; transaction sharding; state sharding***
Near Protocol	1000 TPS	<ul style="list-style-type: none"> <li>Nodes are divided into block producers, validators, and fishermen.</li> <li>Using Nightshade’s sharding method, one block contains all sharded transactions.</li> </ul>	Network sharding; transaction sharding; state sharding
Elrond	10,000 TPS	<ul style="list-style-type: none"> <li>The architecture of MetaChain and shards is adopted.</li> <li>Cross-shard transfer uses an asynchronous model.</li> <li>Dynamically adjusts the number of shards.</li> </ul>	Network sharding; transaction sharding; state sharding

\* To group (shard) the entire blockchain network, and all shards process transactions at the same time to achieve parallel accounting. \*\* To randomly divide the transaction into different shards or groups and let certain nodes conduct accounting. \*\*\* To store complete ledger information in each fragment, and each fragment maintains part of the ledger information.

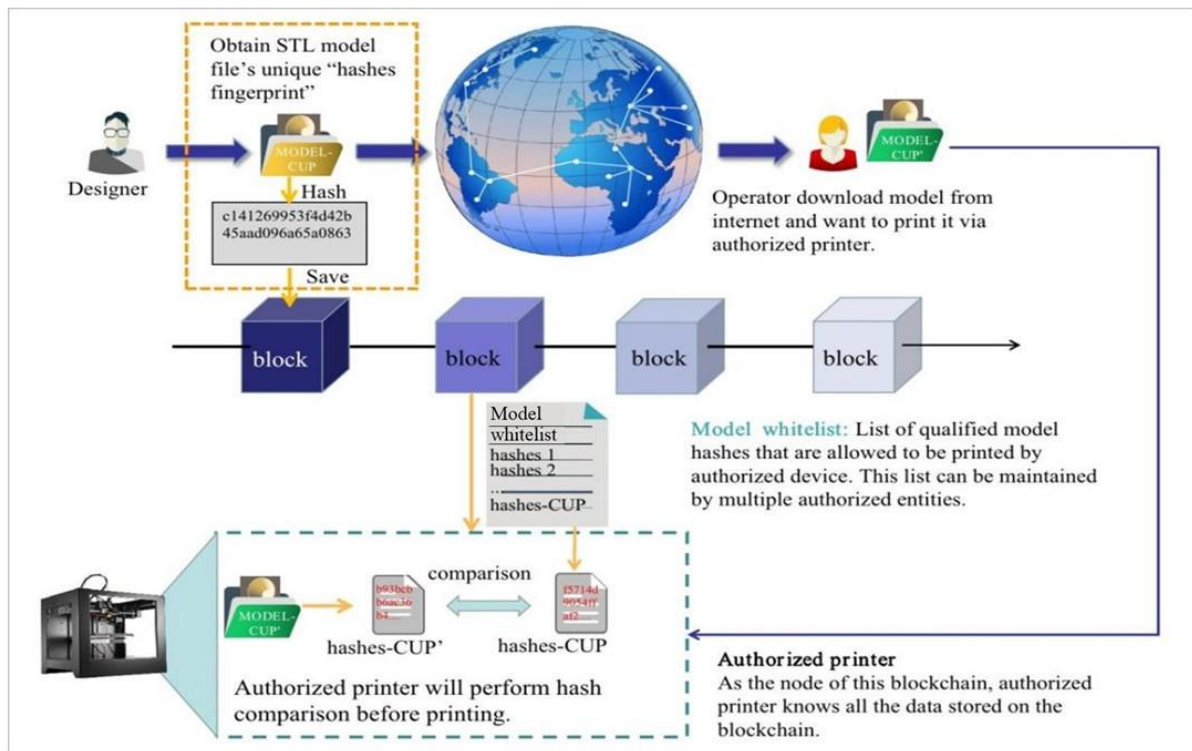
## 2.2. “Fingerprints” of an STL File

The data stored on the blockchain will be saved by nodes, and multiple nodes will have multiple backups. In this way, the blockchain ensures the reliability and security of data. However, 3D models are usually larger than tens of megabytes. If multiple backups are stored in the blockchain, storage resources will be consumed fast.

To solve this storage problem, we use hash function to obtain the “fingerprints” of 3D models and put these “fingerprints” on a blockchain. The term hash function refers to a function that compresses an input bit string of arbitrary length into an output bit string of fixed and finite length [29]. These functions are mainly used to speed up the process of finding stored data. Various files of different sizes, such as videos, email text data, and pictures, can be converted into fixed lengths. The hash function also has unidirectional and anti-collision properties [30]. According to these characteristics, the hash is usually used to ensure data integrity, that is, to verify whether the data are illegally tampered with. Therefore, even if the original data are in an unsafe environment, the integrity of those data can be detected based on their hashes [31]. The hash function can be written as  $y = \text{Hash}(\text{data})$ , where  $y$  is always a fixed-length output. In our case, a hash function is to generate “digital fingerprints” for STL files [32]. If one byte of data is modified in an STL file, completely different hashes will be generated [33].

The 3D model hashing and storage process is shown in Figure 3. In a typical process, the model designer uploads his new design to the system (for convenience, we created a 3D design of a cup named Model-CUP in Figure 3), and the system performs hash calculation and generates the “digital fingerprints” [34]. Later, one operator downloads the Model-CUP from the internet and plans to print it. A 3D model transferred via the internet might not be secured, so the downloaded model was called Model-CUP’. The model file is transmitted over the internet, but its hashes are safely stored on the blockchain. Before printing, an authorized printer which is a node in the blockchain needs to conduct hashes verification and only print these files whose hashes are on the model whitelist. A whitelist is a group of smart contracts on the blockchain [35]. This list is maintained by authorized

multiple entities and updated/changed only allowed when all entities agree with to ensure the credibility of the STL models in the list.



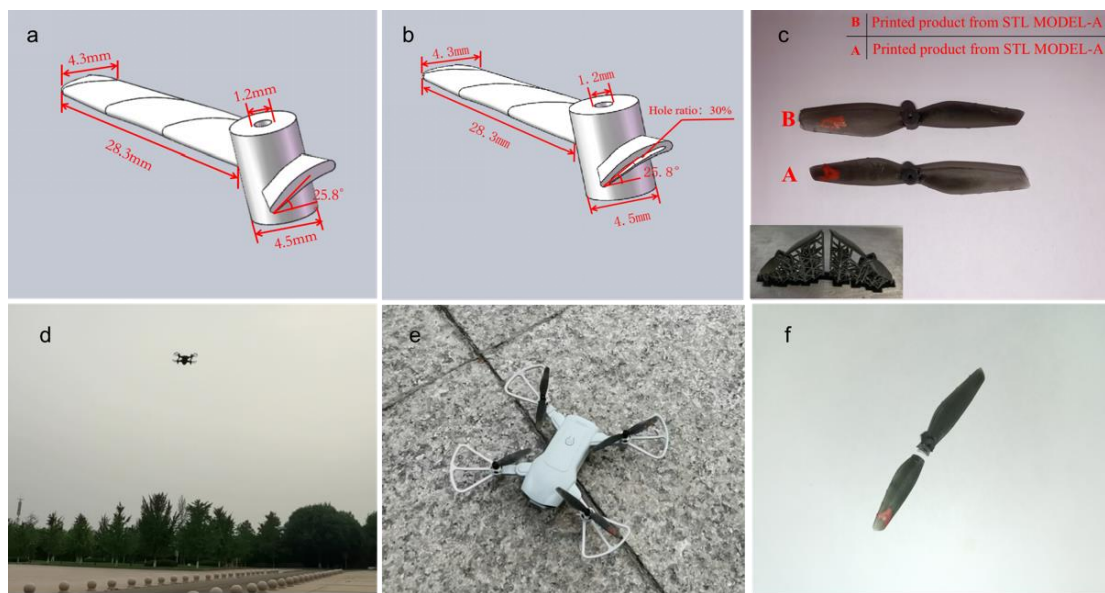
**Figure 3.** The process of hashing 3D model (obtaining the “fingerprints”) and storing “fingerprints” on a blockchain.

### 3. Demonstration and Discussion

To study the feasibility of our design, we designed an attack-defense demo referring to the previously mentioned Dr0wned’s experiment. Firstly, we bought a small UAV from 4DRC (a UAV manufacturer) which was capable to fly for 30 min under normal takeoff conditions, and the blades of this UAV were replicable. Designer Alice drew out the model STL file according to the size of the original blade and stored it on the computer connected to a 3D printer. The 3D printer used here was the photon mono SE light-curing printer from ANYCUBIC. The wavelength of the matrix light source was 405 nm, the Z-axis accuracy was 0.01 mm, the thickness of one layer was 0.01–0.15 mm, and maximum printing speed was 88 mm/h.

Later, hacker Bob (pretended by our lab companion) modified the mentioned drawing. Bob implanted defects into the blade which could lead the fatigue development faster than expected during high-speed rotation. These changes were invisible to the naked eye from only checking the appearance of blades. See Figure 4c, where it is difficult to find out if one of them has a defect. Bob replaced the defective STL file with the genuine one (created by Alice) and all the access and change records were deleted. The original model (Figure 4a), invaded the blade model (Figure 4b), and their printed objects are shown in Figure 4c. To let readers see clearly, we created an obvious defect in Figure 4b, but these modifications can be hidden in a real illegal network intrusion.





**Figure 4.** (a) Model of the original blade (MODEL-A); (b) model of the invaded blade (MODEL-A'). (c) Printed products of MODEL-A (at top, marked as B in picture) and MODEL-A' (at bottom, marked as A in picture). Inert shows these blades were just printed out with supports from stereolithography apparatus. The UAV was flying with implanted defective blades (d). It fell and broke the protective ring (e) and the blade was damaged at the defect (f).

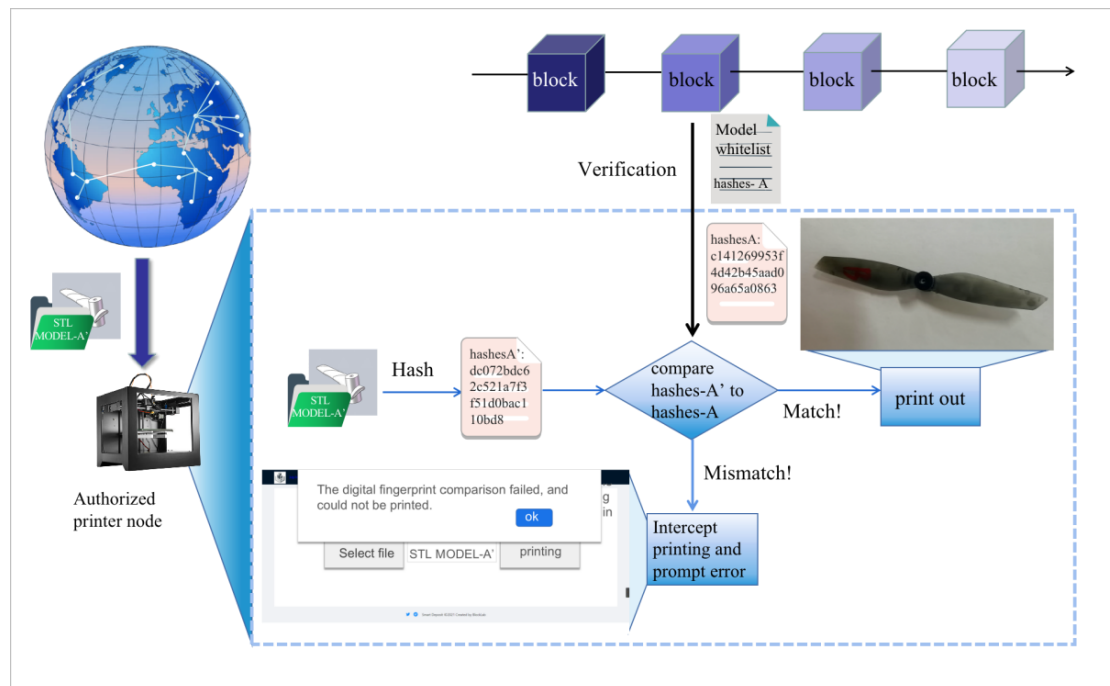
Then, operator Claire printed out the invaded blade model (she did not know this file was invaded) and installed it on the UAV. After normal takeoff, the UAV quickly fell from a 5 m height after the rotor broke, the overall flying time was less than 1 min, and this UAV was damaged (Figure 4d–f). The hacker's tampering affected the flight of the UVA and caused serious damages. As a comparison, if operator Claire printed the right blade model, see Figure 4a, the printed blade can supported flying normally. Under the same meteorological conditions, the UAV can fly at a height of 5 m and safely land after completing various actions instructed by Claire via remote control.

To intercept the illegal blade model invasion, a further defense demonstration was carried out. The key idea is shown in Figure 5. After Bob's attack was complete, operator Claire sent the dummy blade model MODEL-A' to the authorized printer which connected to a blockchain network. This authorized printer obtained the hashes of MODEL-A' firstly and compared them to the 4DRC-UAV parts whitelist, which already included the hashes of approved MODEL-A. This authorized printer only printed out models once their hashes were on the whitelist, and MODEL-A' was not, and the process was terminated.

Through this demonstration, people can believe that the printed products are qualified and from reliable models. Since UAVs may be used to perform important civilian or military missions, it is likely that the design of the UAVs or the credibility of the model may be important. Therefore, it is critical to automatically filter out inappropriate models by the network. In addition, the combination of AM and blockchain can not only reduce labor and time costs but also prevent material waste caused by printing out non-compliant parts. One must avoid misuse due to omission. Verifying the authenticity of drawings can prevent the waste of resources and reduce labor before the inappropriate product is printed.

From the above demonstration, we showed that the STL model without blockchain protection was tampered with and manufactured easily. Problematic products installed on UAVs without verifying will cause UAVs to crash in minutes (as shown in Figure 4d). If the manufacturing scene is oriented to the key components of automobiles and planes, or if problematic products are directly mixed into the supply chain, grave consequences will happen. However, using a blockchain-based "fingerprints" verification process can

intercept these problems and prevent material loss during manufacture. It can prevent counterfeit and inferior components from entering the market.



**Figure 5.** Intercepting the invaded model printing by trusted hash verification.

Our blockchain-based model authentication process relies on a whitelist of printable models, which should be maintained by multiple independent entities via a group of smart contracts running on a blockchain. Independent entities will ensure that their consensus and decisions are reliable and trusted. The whole process mainly includes two key parts: one is creating the printable whitelist and another is verifying before printing.

After receiving an STL model, the network will obtain digital “fingerprints” from original designs and save these “fingerprints” data on a high-performance blockchain. Ideally, to store the model itself on the blockchain directly will be more conducive. However, due to the capacity of the current blockchain, it cannot store large data. Currently, the expansion of the blockchain is a concern of many people, but no breakthrough has been achieved. Therefore, we use a hash function to encrypt the STL model and extract “fingerprints” as an alternative choice.

The hash function is the basis for creating “digital fingerprints” and ensuring security. Through this function, each change in the model will output different “fingerprints” and a blockchain jointly maintained by multiple parties ensures the reliability and security of information on the chain [33]. Creating a whitelist via smart contracts actually adds a double guarantee for the credibility. The “fingerprints” verification commands executed by authorized 3D printers further add a third layer of protection. These three layers can guarantee the security of the model and further ensure the quality and reliability of printed products. Relying on blockchain and smart contracts, a more automated manufacturing process can be established, including recording the designers of 3D printing drawings, where 3D-printed parts are printed, and when the products are printed. It can reduce operating costs, time, and possible human errors. It is also possible to combine “fingerprint” verification with other physical anti-counterfeiting methods, such as embedding anti-counterfeiting codes into physical objects with special materials, further enabling additive manufacturing credibility.

The whitelist is designed to ensure that drawings are credible before printing. Since everyone can upload 3D drawings to the network, only verified designers and drawings can be added into the whitelist (see Listing 1). These actions must be agreed upon by all

the maintainers of the whitelist (such as the signers of the smart contracts). With a reliable whitelist, the verification process is doable. After receiving an instruction to print a model file, the authorized printer extracts “fingerprints” from the just-received file and verifies it (checks within the whitelist). Once the verification process is passed, the authorized printer will print out the model and people can use the printed products without apprehension.

**Listing 1:** Code for maintaining a whitelist of multiple entities.

---

```

contract threedpTrust {
    uint256 constant SIGNATURES = 5;
    address[] manager;
    string[] whiteHash;
    string[] fileHash;
    mapping(string => uint256) private signatureNum;
    mapping(string => bool) private hashExisted;
    mapping(string => bool) private hashIsWhite;
    mapping(string => mapping (address => bool)) private notVote;
    modifier onlyManager {
        require(msg.sender == manager[0] || msg.sender == manager[1] || msg.sender == manager[2]
        || msg.sender == manager[3] || msg.sender == manager[4]);
        _;
    }
    modifier notExisted(string memory _fileHash) {
        require(hashExisted[_fileHash] == false);
        _;
    }

    constructor(
        address _firstManager,
        address _secondManager,
        ...
    ) {
        manager[0] = _firstManager;
        manager[1] = _secondManager;
        ...
    }

    function uploadHash(string memory _fileHash) public notExisted(_fileHash) returns(bool) {
        fileHash.push(_fileHash);
        signatureNum[_fileHash] = 0;
        hashExisted[_fileHash] = true;
        hashIsWhite[_fileHash] = false;
        return true;
    }

    function signHash(string memory _fileHash) public onlyManager returns(bool) {
        require(notVote[_fileHash][msg.sender] == false, "You have already signed this file hash");
        notVote[_fileHash][msg.sender] = true;
        if (signatureNum[_fileHash] == 5) {
            whiteHash.push(_fileHash);
            hashIsWhite[_fileHash] = true;
        } else {
            signatureNum[_fileHash] += 1;
        }
        return true;
    }

    function checkHash(string memory _fileHash) public view returns(bool) {
        return hashIsWhite[_fileHash];
    }

}

```

---



In our future work, we plan to expand the existing solution to ensure the reliability of 3D-printed products by combining digital fingerprints, physical anti-counterfeiting methods, and online printing together. Users can choose to print 3D drawings without direct contact with the original drawings. The formed product comes with an integrated label for tracking and recording the scanning data (number of times, time, scanning location, etc.) of the 3D-printed product, which will improve the credibility of 3D printing.

The wide use of 3D printing has brought the possibility of cybercrime, especially invading 3D models to destroy the printed product during the additive manufacturing process. More and more enterprises have noticed this problem. General Electric stated in its patent application, “If a replacement for an industrial asset can be produced by an additive manufacturing process, then any user of appropriately configured additive manufacturing equipment can replicate the part [36].” Potential solutions to solve this problem (counterfeit and product quality degradation) may attract the attention of large manufacturing companies. Later, some obvious indicators may reflect changes from using blockchain technology. For example, infringement cases and models which are tampered with have been greatly reduced after using our method.

In fact, blockchain can not only protect models for additive manufacturing but also will greatly save industrial maintenance costs. For example, an aircraft component provider, Moog, demonstrated an interesting case of using blockchain [37]. ST Aerospace purchased a digital model of an aircraft replacement part from Moog and printed the part at its facility in Singapore. The whole process was digital and the settlement was instantaneously completed via a smart contract on Microsoft’s Azure blockchain. There is no doubt that the combination of blockchain and additive manufacturing has great potential.

#### 4. Conclusions

In the field of additive manufacturing, a great deal of research has been conducted on developing new printing principles, process management, and equipment upgrades. However, extensive research on information security, license management, copyright protection, and proof of authenticity in additive manufacturing remain seriously insufficient. In particular, model data transmission dominates the security and risk management of the entire system. The security of drawings used for printing is very important and worthy of attention.

This work shows how to protect 3D models from invading and prove the authenticity of the printed objects via blockchain. The “fingerprint” of a model is extracted by a hash algorithm. This “fingerprint” can be saved on a blockchain. Relying on sharding technology, a high-throughput blockchain network can be used to verify models with high efficiency. Our method can resist tampering, effectively ensuring the safety of STL files in the digital world through a specific demonstration.

**Author Contributions:** Conceptualization, Y.W. and Y.Y.; validation, Y.W., S.S. and M.W.; writing—original draft preparation, Y.W.; supervision, Y.Y. and W.R. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research was funded by the National Science Foundation of China under grant numbers 51831010 and 12174210; the Innovation Team Project of Ji’nan, grant number 2019GXRC035.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Exclude this statement.

**Acknowledgments:** This work is supported by the National Science Foundation of China (Grant Nos. 51831010 and 12174210) and the Innovation Team Project of Ji’nan (Grant No. 2019GXRC035).

**Conflicts of Interest:** The authors declare that they have no known competing financial interest or personal relationship that could have appeared to influence the work reported in this paper.

## References

1. Booyens, G.J.; Van der Merwe, A.F.; De Beer, D.J. Additive manufacturing for sustainable custom-designed implants. *S. Afr. J. Ind. Eng.* **2019**, *30*, 21–31. [CrossRef]
2. Bachhar, N.; Gudadhe, A.; Kumar, A.; Andrade, P.; Kumaraswamy, G. 3D printing of semicrystalline polypropylene: Towards eliminating warpage of printed objects. *Bull. Mater. Sci.* **2020**, *43*, 171. [CrossRef]
3. Salmi, M. Additive manufacturing processes in medical applications. *Materials* **2021**, *14*, 191. [CrossRef] [PubMed]
4. Lin, C.; Chen, T. 3D printing technologies for enhancing the sustainability of an aircraft manufacturing or MRO company—A multi-expert partial consensus-FAHP analysis. *Int. J. Adv. Manuf. Technol.* **2019**, *105*, 4171–4180. [CrossRef]
5. Pervaiz, S.; Qureshi, T.A.; Kashwani, G.; Kannan, S. 3D printing of fiber-reinforced plastic composites using fused deposition modeling: A status review. *Materials* **2021**, *14*, 4520. [CrossRef]
6. New Wohlers Report 2021 Finds 7.5% Growth in Additive Manufacturing Industry Despite Pandemic. Available online: <https://wohlersassociates.com/press83.html> (accessed on 21 November 2021).
7. Security Alert: 3D Printing-Counterfeit High Security Bolt Seals. Available online: <https://blog.gwccnet.com/blog/security-alert-3d-printing-counterfeit-high-security-bolt-seals> (accessed on 21 November 2021).
8. Shanghai Police Destroy a Criminal Gang that Manufactures and Sells Counterfeit Ultraman Toys, the Amount Involved Is More than 4 Million Yuan. Available online: <http://lfjx.samr.gov.cn/article/yasf/202109/3640.html> (accessed on 21 November 2021).
9. Belikovetsky, S.; Yampolskiy, M.; Toh, J.; Gatlin, J.; Elovici, Y. Dr0wned—Cyber-physical attack with additive manufacturing. In Proceedings of the 11th {USENIX} Workshop on Offensive Technologies ({WOOT} 17) 2017, Vancouver, BC, Canada, 14–15 August 2017. Available online: <https://www.usenix.org/system/files/conference/woot17/woot17-paper-belikovetsky.pdf> (accessed on 21 November 2021).
10. Abdallah, M.; Hijazi, A.; Graff, B.; Fouassier, J.; Rodeghiero, G.; Gualandi, A.; Dumur, F.; Cozzi, P.G.; Lalevée, J. Coumarin derivatives as versatile photoinitiators for 3D printing, polymerization in water and photocomposite synthesis. *Polym. Chem.* **2019**, *10*, 872–884. [CrossRef]
11. Qiu, W.; Zhu, J.; Dietliker, K.; Li, Z. Polymerizable oxime esters: An efficient photoinitiator with low migration ability for 3D printing to fabricate luminescent devices. *ChemPhotoChem* **2020**, *4*, 5296–5303. [CrossRef]
12. Ts, A.; Qi, Z.A.; Tao, Z.B.; Xsa, C.; Jgl, D. Co-doping Mn 2+ /Cr 3+ in ZnGa 2 O 4 to fabricate chameleon-like phosphors for multi-mode dynamic anti-counterfeiting. *Chem. Eng. J.* **2021**, *426*, 131744.
13. Eisenbarth, D.; Stoll, P.; Klahn, C.; Heinis, T.B.; Wegener, K. Unique coding for authentication and anti-counterfeiting by controlled and random process variation in L-PBF and L-DED. *Addit. Manuf.* **2020**, *35*, 101298. [CrossRef]
14. Zhang, C.; Li, H.; Chen, X.; Shi, X. Research on watermark printing technology of STL model based on Menger curvature. In Proceedings of the 2021 4th International Conference on Advanced Algorithms and Control Engineering (ICAACE 2021), Sanya, China, 29–31 January 2021; p. 12075.
15. Yan, C.; Zhang, G.; Wang, A.; Liu, L.; Chang, C. Visible 3D-model watermarking algorithm for 3D-Printing based on bitmap fonts. *Int. J. Netw. Secur.* **2021**, *23*, 172–179.
16. Cao, J.; Niu, Z.; Wang, A.; Liu, L. Reversible visible watermarking algorithm for 3D models. *J. Netw. Intell.* **2020**, *5*, 129–140.
17. Gao, Y.; Wang, W.; Jin, Y.; Zhou, C.; Xu, W.; Jin, Z. ThermoTag: A hidden ID of 3D printers for fingerprinting and watermarking. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 2805–2820. [CrossRef]
18. Laftah, M.M. Watermarking of a 3D Model based on Wavelet Transform. *Iraqi J. Sci.* **2021**, *62*, 4999–5007. [CrossRef]
19. Feng, X.; Li, L.; Wang, J.; Dong, K.; Liu, Y.; Yan, S. Research progress on copyright protection technology of 3D printing model. *Chin. J. Image Graph.* **2019**, *24*, 1028–1041.
20. Kurpuweit, S.; Schmidt, C.G.; Klöckner, M.; Wagner, S.M. Blockchain in additive manufacturing and its impact on supply chains. *J. Bus. Logist.* **2021**, *42*, 46–70. [CrossRef]
21. Alkhader, W.; Alkaabi, N.; Salah, K.; Jayaraman, R.; Arshad, J.; OMAR, M. Blockchain-Based Traceability and Management for Additive Manufacturing. *IEEE Access* **2020**, *8*, 188363–188377. [CrossRef]
22. Yang, D.; Long, C.; Xu, H.; Peng, S. A review on scalability of blockchain. In Proceedings of the 2020 2nd International Conference on Blockchain Technology, Hilo, HI, USA, 12 March 2020; pp. 1–6.
23. Grodzicka, H.; Kedziora, M.; Madeyski, L. Security and scalability in private permissionless blockchain: Problems and solutions leading to creating Consent-as-a-Service (CaaS) deployment. In Proceedings of the International Conference on Computational Collective Intelligence, Rhodes, Greece, 27 September 2021; pp. 278–289.
24. Shahsavari, Y.; Zhang, K.; Talhi, C. A theoretical model for block propagation analysis in bitcoin network. *IEEE Trans. Eng. Manag.* **2020**, *69*, 1459–1476. [CrossRef]
25. Dang, H.; Dinh, T.T.A.; Loghini, D.; Chang, E.; Lin, Q.; Ooi, B.C. Towards scaling blockchain systems via sharding. In Proceedings of the 2019 International Conference on Management of Data, Amsterdam, The Netherlands, June 30–July 5 2019; pp. 123–140.
26. Shevkar, R. Performance-based analysis of blockchain scalability metric. *Tehnički Glasnik* **2021**, *15*, 133–142.
27. Wang, G.; Shi, Z.J.; Nixon, M.; Han, S. Sok: Sharding on blockchain. In Proceedings of the 1st ACM Conference on Advances in Financial Technologies, Zurich, Switzerland, 21–23 October 2019; pp. 41–61.
28. Zhou, Q. *Boson Consensus: A Scalable Blockchain Consensus Algorithm*; Quark Chain Foundation Ltd.: Singapore, 2019; pp. 1–18.
29. Abdoun, N. *Design, Implementation and Analysis of Keyed Hash Functions Based on Chaotic Maps and Neural Networks*; Nantes: Nantes, France, 2019.

30. Wang, B.; Li, S. Research of combining blockchain in the course reform of cryptography by experiential teaching. In Proceedings of the 2021 9th International Conference on Information and Education Technology (ICIET), Okayama, Japan, 27–29 March 2021; pp. 133–138.
31. Zhai, S.; Yang, Y.; Li, J.; Qiu, C.; Zhao, J. Research on the Application of Cryptography on the Blockchain. *J. Phys. Conf. Ser.* **2019**, *1168*, 32077. [[CrossRef](#)]
32. Cai, X.Q.; Deng, Y.; Zhang, L.; Shi, J.C.; Chen, Q.; Zhen, W.L.; Liu, Z.Q.; Long, Y.; Wang, K.; Li, C. The principle and core technology of blockchain. *Chin. J. Comput.* **2019**, *42*, 1–15.
33. Mandolla, C.; Petruzzelli, A.M.; Percoco, G.; Urbinati, A. Building a digital twin for additive manufacturing through the exploitation of blockchain: A case analysis of the aircraft industry. *Comput. Industry* **2019**, *109*, 134–152. [[CrossRef](#)]
34. 3DPTrust. Available online: <http://www.3dptrust.com/home?s=%2Fhome> (accessed on 24 January 2022).
35. Bhardwaj, A.; Shah, S.B.H.; Shankar, A.; Alazab, M.; Kumar, M.; Gadekallu, T.R. Penetration testing framework for smart contract blockchain. *Peer* **2021**, *14*, 2635–2650. [[CrossRef](#)]
36. Industrial Giant GE Eyes Blockchain in Fight Against 3D-Printing Fakes. Available online: <https://www.coindesk.com/industrial-giant-ge-eyes-blockchain-in-fight-against-3d-printing-fakes/> (accessed on 21 November 2021).
37. Moog and ST Aerospace to Collaborate on Industry’s First: Blockchain and 3D Printing-Enabled Total Digital Transaction. Available online: <https://www.stengg.com/en/newsroom/news-releases/moog-and-st-aerospace-to-collaborate-on-industry-s-first-blockchain-and-3d-printing-enabled-total-digital-transaction/> (accessed on 21 November 2021).