IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 3, 2021, accepted May 10, 2021, date of publication May 20, 2021, date of current version June 2, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3082215

Efficient and Secure Blockchain System for Digital Content Trading

GABIN HEO[1], DANA YANG[2], INSHIL DOH[3], AND KIJOON CHAE[2]
[1]Division of Artificial Intelligence and Software, Ewha Womans University, Seoul 03760, South Korea
[2]Department of Computer Science and Engineering, Ewha Womans University, Seoul 03760, South Korea
[3]Department of Cyber Security, Ewha Womans University, Seoul 03760, South Korea

Corresponding author: Kijoon Chae (kjchae@ewha.ac.kr)

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea Government [Ministry of Science and ICT (MSIP)] under Grant NRF-2019R1F1A1063194 and Grant NRF-2020R1A2C1006497.

ABSTRACT Blockchain is attracting attention as a new solution for problems such as illegal copying, profit distribution, and forgery and falsification in the digital content trading environment, which has become an essential asset in the information age. However, one problem is that it is difficult to propagate digital content to the blockchain network because of a limited capacity to upload to the blockchain. The integrity and transparency of blockchain are also considered as weak points in terms of privacy. In this paper, we propose a new blockchain system, the secret block-based blockchain (SBBC), to address the problems with the blockchain system in the digital content trading environment. SBBC is composed of off-chain and on-chain network components. Off-chain is the part that allows trading digital content through the authentication phase. The digital content that is traded has a digital fingerprint inserted, so if an illegal leak occurs, the destination can be tracked. In addition, the content is encrypted and traded, and only the rightful user can use the digital content, thus ensuring income for the legitimate content author. Next, the on-chain network is licensed to use digital content, and a verification process using a consensus algorithm is performed. The licensed consumer creates a secret block of their transaction and records it only on their ledger. In a private part, secret block creation ensures privacy and solves the network overload that can occur when uploading digital content to the blockchain. Finally, through the verification and agreement of all blockchain participants, a public block is created and recorded in the ledger to finalize the transaction. Consequently, we propose the SBBC system suitable for digital content trading environments and a safe and reliable system through a consensus algorithm in such environments.

INDEX TERMS Blockchain, digital content trading, privacy, DRM, digital fingerprinting, secret block, consensus algorithm.

I. INTRODUCTION

With the recent development of the Internet of Everything (IoE), all information shared over a network, information has become an important resource. In particular, virtual reality (VR), augmented reality (AR), and mixed reality (MR) digital content has appeared, as well as movies and music. This allows interaction between ''virtual'' and ''real,'' and users can have new experiences through digital content. The scale and prospects of digital content are expected to increase gradually due to smart devices and platform service expansions by global companies. However, conventional digital content trading environments have problems with illegal copying and leaking, profit distribution, forgery, and falsification. The current digital content market growth rate is slow because of these problems [1], [2]. Various mechanisms to solve these problems and protect digital content have been proposed, including digital rights management (DRM) and digital fingerprinting, which track illegal actions [3]. However, even with these technologies, various problems remain, including profit distribution, forgery, and falsification. Therefore, studies applying blockchain to digital content trading environments have attracted attention as a core technology for the fourth industrial revolution [4]. Blockchain as a peer-to-peer (P2P) based distributed open ledger can ensure transparency, data integrity, and high security for all participants contributing transaction information to the ledger. Because transactions are processed without third-party input, the transaction reliability is high. Problems with the current digital content trade can be solved by applying a blockchain with these characteristics to the digital content environment. However, because there is little capacity for uploaded content to the

The associate editor coordinating the review of this manuscript and approving it for publication was Neetesh Saxena.

blockchain, it is technically difficult to upload digital content such as videos. In addition, because all participants should have a transaction ledger, anyone can confirm sensitive information included in the transaction, which leads to personal information leakage [5]. This can be solved by taking advantage of distributed ledgers and P2P communication by integrating blockchain technology with illegal leakage and profit distribution that appear indiscriminately in traditional digital content trading environments. However, this is unsuitable for incorporating current blockchain systems in digital content trading environments because it does not consider problems occurring in the blockchain. This paper analyzes the current digital content trading environment and blockchain problems and proposes the secret block-based blockchain (SBBC) system to solve them. Secret blocks (SBs) solve storage space limitations and personal information leakage that are problematic in current blockchains. Considering digital content trading environment characteristics, this work proposes a weighted authentication byzantine fault tolerance (WBFT) algorithm, an authentication mechanism that assigns a high weight for authentication [6]. The main contributions of this paper can be summarized as follows.

- We investigated problems with integrating the appropriate blockchains with digital content trading environments. Consequently, we confirmed that blockchain, which has attracted attention as a new mechanism for digital content trading, has various problems, including privacy issues.
- We propose SBBC, a blockchain system suitable for digital content trading environments. Because SBBC creates SBs, it solves the privacy and storage capacity limitation problems in current blockchains.
- We propose WBFT, a weight-based consensus algorithm for SBBC. WBFT is a consensus algorithm tailored to the SBBC environment cohabited by authenticated and unauthenticated users. Reliable consensus is achieved by setting larger authenticated user weights.
- We simulated the proposed consensus algorithm and blockchain environment, and we confirmed that consensus was reached more quickly than with the current consensus algorithm, and it was more efficient when analyzing latency and throughput in the blockchain.

The remainder of this paper is organized as follows. Section II analyzes traditional blockchain and consensus algorithms, and Section III examines the proposed SBBC overall structure. Section IV compares consensus performance for the current and proposed WBFT consensus algorithms and analyzes SBBC efficiency and security. Finally, Section V concludes this paper by discussing our implications and future research.

II. RELATED WORK

A. DIGITAL CONTENTS

Digital content has become an essential asset with new business developments, such as video streaming platforms and internet broadcasting platforms. Thus, market size and demand for digital content have also increased significantly, but digital content trading environments have several problems [7].

- *Illegal copying and leakage:* Offline illegal copying has significantly decreased with digital content consumption environment changes to downloading and streaming. However, illegal copy distribution on the network is increasing, with torrent and social networking services becoming the main distribution path for illegal copies [8]. To solve this problem, only users with legitimate rights should be able to use digital content.
- *Profit distribution:* Some current content associations operate a trust management system as an intermediary to protect content creator rights. However, revenue returned to the content creators is relatively small due to unequal profit distribution and high fees [9]. To solve this problem, the system needs to ensure digital content payments go directly to content creators without third-party intervention.
- *Forgery and falsification:* Digital data, such as digital content and software, can be easily modified or copied; hence, forgery and falsification problems are rife [10]. Although anti-copying technologies such as watermarking are available, they have various limitations in blocking forgery and falsification at the source. To solve this problem, the system needs to check the digital content integrity and validity by recording the content information and details.

Various mechanisms to address these problems and protect digital content have been proposed, including DRM and digital fingerprinting, which are used in this paper.

1) DIGITAL RIGHTS MANAGEMENT

DRM allows only legitimate users to access content, preventing illegal copying of copyrighted work. DRM employs usage rules and content encryption to control and restrict content usage [11]. Usage rules control the number of installations, use periods, and digital content transfer rights according to the user's purchased content, and DRM ensures that users can only access digital content after selecting and paying for the appropriate usage rule. Content encryption provides users who have made a legitimate purchase with a decryption key to enable access only to content the user has paid for [12]. The DRM components include protected content, users with access, and licenses or rules for use permission. The content server applies DRM to digital content and generates packaged content, providing copyright protection, and distributes it to users. The server is responsible for issuing and managing licenses according to rules the user requests (such as period of use and number of installations). The DRM client controls digital content use according to the license issued by the user. Content may be used after the license is issued by the DRM server, releasing packaged content copyright protection issued by the content server. Thus, DRM offers a mechanism to authenticate user activity because the content

TABLE 1. Requirements and proposed solutions to blockchain problems.

problem	Explanation	Requirement	Solution
Private blockchain abuse	Ease makes malicious actions such as abuse of authority and counterfeiting transactions more prevalent than on public blockchains	Construct an environment where a large number of participants participate, including the operating entity	Network configuration with various participants
False transactions and network overload	False transaction validation increases processing time and results in network overload	Design an authentication protocol to prevent false transactions due to anonymity	User authentication
Storage space limitations	When attaching a large amount of data, it must be replicated to all nodes, leading to network overhead	Ensure only the user who made the transaction has access to the content	Secret blocks
Privacy	Because transaction information is recorded in a block, it is difficult to implement the "right to be forgotten," and data deletion cannot be guaranteed	Design a privacy protection mechanism where only the trading party confirms the transaction	SBBC

is protected in an encrypted form, and the user is issued a package with a license and decryption key only after making a legitimate payment. In particular, DRM blocks access from unauthorized users and manages digital content usage within the range of rights granted to users, thereby satisfying the continuous protection of digital assets.

2) DIGITAL FINGERPRINTING

Digital fingerprinting is a steganographic technique that originated to hide secret information in pictures or letters. Recently, it has been used for digital content. Steganography is used to prevent illegal copying and protect the content owner's copyright by embedding identifiers in media such as videos and photos [13]. Digital watermarking is used to claim content ownership by inserting an identifier with information about the copyright holder, whereas digital fingerprinting can track the source of an illegal content leak by inserting an identifier with information about the user who received the content. Various information can be inserted as an identifier, such as copyright information and images. Identifiers are generally inserted so that humans cannot detect them. Digital fingerprinting technology needs to provide not only authenticated ownership but also user identification; hence, other features are required in addition to current digital watermarking requirements.

B. BLOCKCHAIN

Blockchain is a distributed system that emerged as a solution to security threats and high management costs for centralized systems. Participants collectively record and manage transactions in a decentralized network. Data reside in a block in P2P-based distributed open-ledger blockchains, where each block is connected and stored in chain form using hash values [14]. Blocks are divided into block headers and block bodies. Block headers include the version, Merkle root, block creation time, mining difficulty, and previous block hash value. Each block is connected to the previous block by holding the previous block's hash value. Transactions are stored in the block body, allowing blockchain network participants to verify wallet addresses and transaction amounts for recipients and senders, ensuring data integrity and transparency.

1) BLOCKCHAIN PROBLEMS ANALYSIS

Blockchains have been proposed to solve digital content trading environment problems, but some problems remain. This paper analyzes known blockchain problems shown in Table 1 and considers a blockchain system suitable for digital content trading [15]. Blockchains are divided into public and private blockchains. Public blockchains agree with the participant majority; hence, malicious activity is possible if someone controls more than 51% of nodes, called a 51% attack. However, 51% attacks on public blockchains are considered to be practically impossible due to the required infrastructure cost. On the other hand, private blockchains are operated by an operating body, such as a regulatory body or operating committee; hence, it is possible to take malicious action by seizing the operating entity or stealing the authority. Therefore, to prevent the occupancy of the blockchain by a small number of malicious users, it is necessary for many users, including the operating entity, to participate in the blockchain. This paper considers a public blockchain with various participants as the basic structure to prevent problems with the blockchains, such as rights abuse and transaction counterfeiting.

Several problems arise when using a public blockchain. Private blockchains can take immediate action, such as blocking participants that cause suspicious transactions from the network. In contrast, public blockchain anonymity shields participants' transactions and verifications and hence can allow false transactions, increasing the wait time for real transactions and leading to network overload. Therefore, we propose including a mechanism for user authentication to prevent false transactions. Furthermore, all blockchains

have storage limitations, but they also require that all nodes record and have the same information in the ledger. Hence, if a large amount of data is attached to a block, it must be replicated among all the nodes, which can also lead to network overhead. Thus, there is a limit to the content size that can be uploaded to the blockchain, creating a technical problem applying blockchain for digital content trading, such as sound sources, VR, or video. We solve this by setting large data volumes to be owned only by the trading party, with only the metadata recorded on the blockchain and distributed. Therefore, digital content is recorded only in the consumer's ledger through SBs, and the SB information is copied to all nodes to reduce network overhead [16]. Finally, a critical privacy requirement for the recently established General Data Protection Regulation (GDPR) in Europe is to comply with IT system privacy concepts. Blockchain guarantees transparency because anyone in the network can check transaction information, which is somewhat weak regarding personal information security [17]. It is also impossible to guarantee data deletion because the blocks are chained and distributed. Therefore, a mechanism is required to protect privacy such that only the trading party can confirm transactions [18]. We propose a safe and reliable technique to achieve this using a SB-based blockchain system.

2) BLOCKCHAIN CONSENSUS ALGORITHMS

Blockchain is a distributed ledger system where many nodes are connected to a P2P network to verify and record transaction information. Information delay and non-arrival cannot be avoided in P2P networks. Therefore, even if there is no intention to falsify data, there is a risk of duplicate processing due to double transmission and malfunction caused by incorrect information. We propose a consensus algorithm to solve these problems [19]. Proof of work (PoW) is a representative consensus algorithm for public blockchains that has become widely known from its Bitcoin application. The first person to solve a specific problem through computer computation is granted the right to create a block [20]. However, PoW is based on who consumed how much energy and solved the problem, and hence it can be quite inefficient under some conditions. We also considered the proof of stake (PoS) consensus algorithm, which grants authority to create blocks in proportion to the amount at stake rather than computing power, helping to prevent computing and electrical power waste [21]. However, because PoS verifies block validity by stake size, there is a problem with the ''rich getting richer and the poor getting poorer''; that is, decisions tend to be made by a small number of people with large stakes. Practical byzantine fault tolerance (PBFT) is a consensus algorithm that solves PoW and PoS speed and performance problems, can achieve consensus even in an asynchronous network, and can accommodate any number of traitor nodes in the network while ensuring trust to achieve successful consensus [22]. Decisions are made through communication with all nodes; hence, it is commonly employed for private blockchain. PBFT is faster than the public blockchain consensus algorithm and ensures fairness because all nodes communicate. However, although PBFT ensures fairness, the verification rate is reduced as the number of nodes increases, hence reducing transaction throughput. To solve this problem with PBFT, an improved algorithm has been developed. T-PBFT uses EigenTrust to calculate the trust value of each node to increase the consensus efficiency [23]. It selects a node with a high trust value to proceed with the PBFT consensus algorithm. This algorithm is suitable for consortium blockchain or private blockchain because it must calculate all the trust values between nodes. G-PBFT is an improved PBFT algorithm suitable for Internet of Things (IoT) environments. G-PBFT uses the geographical information of IoT devices to ensure the loyalty of the endorsers and increases security by preventing sybil attacks [24]. Because G-PBFT uses geographic information to reach consensus, IoT devices periodically transmit their locations. This is suitable for consensus algorithms for data security in IoT environments but not for digital content trading environments. This is because, in the digital content trading environment, mechanisms such as DRM and digital fingerprinting are already used for the security of digital content, so there is no need to communicate additional location information for data security.

Therefore, in this work, we intend to reduce resource costs and improve execution time by employing PBFT, which solves the PoW and PoS algorithm performance problems for public blockchains. However, the communication level depends on the number of nodes, and public blockchains have many nodes. Therefore, we propose a specific algorithm suitable for the digital content trading environment using public blockchain to solve the problem.

III. SBBC FOR DIGITAL CONTENT-TRADING ENVIRONMENT

A. SBBC OVERALL STRUCTURE

This paper proposes SBBC using the WBFT algorithm, which assigns weights depending on whether a user is authenticated [6]. The SBBC is defined as off- and on-chain to graft a blockchain system suitable for digital content trading. The basic structure follows public blockchain and guarantees transparency and integrity through the environment. SBs solve blockchain problems to provide a safe and reliable system for digital content trading. Figure 1 shows the proposed SBBC system overall structure. Authentication is performed in SBBC off-chain before the digital content is traded, and only authenticated users can proceed with the digital content trading. Licensing to use DRM content is performed in SBBC on-chain. Users who purchase digital content generate transaction records as SBs, and agreements are made by a number of validators on the public blockchain. Figure 2 shows the proposed SBBC process not only resolves problems in the digital content trading environment but also improves privacy and limited capacity problems that arise when integrating blockchain. Table 2 describes the symbols used in Figure 2 and Figure 3.

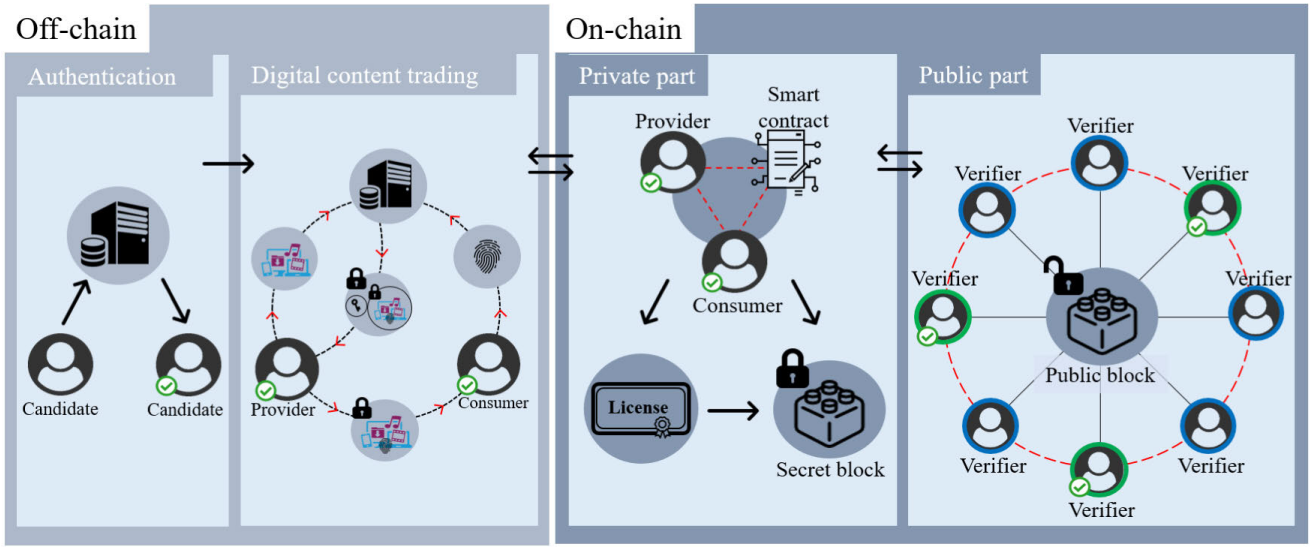


FIGURE 1. Proposed SBBC structure.

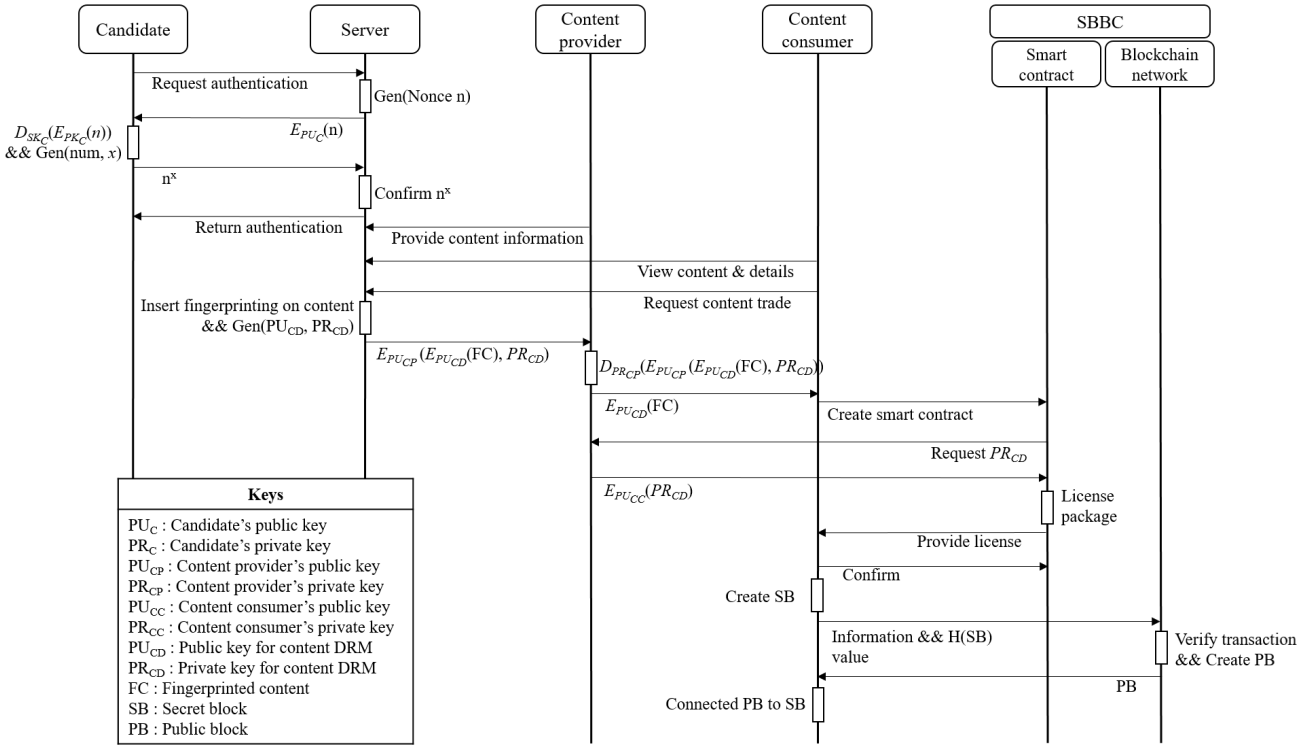


FIGURE 2. SBBC sequence from user authentication to transaction creation and consensus in the blockchain network.

B. OFF-CHAIN COMPONENTS OF THE SBBC

1) USER AUTHENTICATION

Anyone can participate in current public blockchain transactions and obtain verification without authentication. There is no limit to participation, transparency is high, and integrity is guaranteed because many users have transaction records. However, anonymity allows malicious behavior, often in the form of false transactions. This increases the waiting time for legitimate transaction verification because the public blockchain verifies all transactions, and it ultimately leads to system network overload. The proposed SBBC resolves this problem by performing user authentication off-chain before the transaction. Anyone can verify it, but authentication must be completed to prevent false transactions. Any individual who wants to sell or use digital content among the SBBC participants must go through the corresponding authentication process. Figure 3 shows the authentication process. First, the user goes through a registration process. The user sets

TABLE 2. Description of the symbols used in the sequence and Schnorr protocol.

Symbol	Description
PU_C	Candidate's public key
PR_C	Candidate's private key
PU_S	Server's public key
PU_{CP}	Content provider's public key
PR_{CP}	Content provider's private key
PU_{CC}	Content consumer's public key
PR_{CC}	Content consumer's private key
PU_{CD}	Public key for content DRM
PR_{CD}	Private key for content DRM
FC	Fingerprinted content
E_{key}	Encryption with key
D_{key}	Decryption with key
n	Nonce value
x	Random value selected from PW hash values
num	Random number
p	Prime number
q	Prime number ($p-1$ factor)
a	Parameter used to calculate v
v	Public key
s	License hash value
r	Random number
M	SB hash value
e, y	Schnorr signature

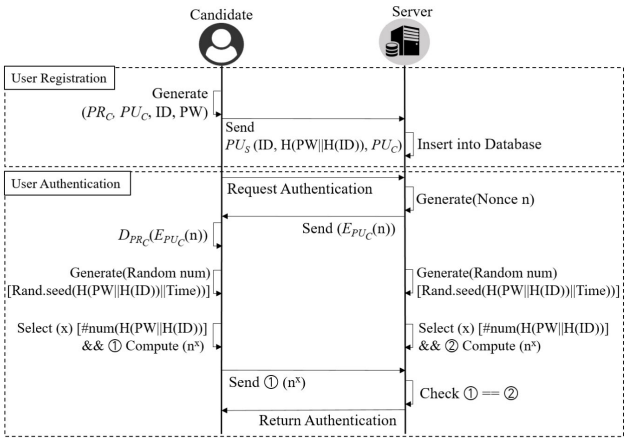


FIGURE 3. SBBC user authentication process.

their ID and password (PW), generates an asymmetric key, then generates a hash value from their PW and the ID hash value and stores the ID, PW hash value, and public key on the server. Subsequently, registered users go through an authentication process when they want to make a transaction. When the user sends an authentication request to the server, the server generates a random number, encrypts it with the user's public key, and transmits it. The user verifies the random number by decrypting the cipher text with their private key. The server and user generate a random value using the value that connects the PW hash value and the authentication request time as a random seed. The value x is selected using the corresponding random value for the PW hash value. Then, a random number n is calculated to the power of x and transmitted to the server. If the value is the same, the server determines that the user is legitimate and completes the authentication. Because the random number is encrypted and transmitted with the user's public key, a user without the private key cannot decrypt the random number required for authentication. Duplicating the random value is prevented by including the authentication request time in the random seed. Thus, the random value cannot be derived, the value of x cannot be calculated, and a secure authentication cannot be performed.

2) DIGITAL CONTENT TRADING

Digital content is more suited to various processing methods than analog content, and it is much easier to merge content. However, these advantages also create problems with illegal copying and leaking, which has only recently been resolved. Encryption is performed to use DRM in the off-chain digital content trading area; that is, only users with legitimate rights to the digital content can use it. However, the content must be decoded into its original state for the user to access it, creating an unsafe section where the content exists in the original state. This can potentially allow illegal content leakage. Therefore, digital fingerprinting is incorporated into the decoded content to trace any leakage [25]. First, the authenticated content provider transmits their content to the server. A consumer who wants to use the content goes through authentication and requests a transaction from the server. The server generates an asymmetric key to apply DRM and then performs a fingerprinting operation using the stored user information. At this time, refer to Figure 4, fingerprinting is inserted as follows.

1) The content server subdivides content into arbitrary sizes and bits.
2) The server randomly determines where and how many fingerprints will be inserted among the subdivided bits.
3) The server inserts the fingerprinting in the designated location.

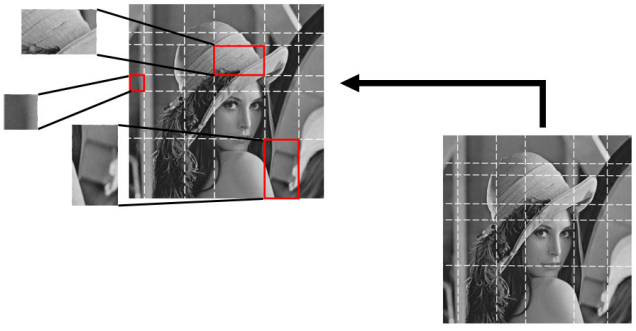


FIGURE 4. Digital fingerprinting application to prevent the possibility of illegal copying and leaking of digital content.

This prevents the user from knowing where the fingerprint is inserted. Content containing the fingerprint is encrypted

through the public key generated for DRM. The server then encrypts the encrypted content, the private key to decrypt the content, and the consumer's public key using the content provider's public key, and it transmits the content to the content provider. The content provider then transmits the encrypted content to the consumer when they accept the consumer's transaction request. The possibility of illegal copying and leaking is prevented through digital content trading in this order. In addition, it is possible to solve the problem of damaging and leaking content by inserting fingerprints in random places and numbers. Therefore, after safely transacting in the off-chain digital content trading area, the on-chain area will proceed.

C. ON-CHAIN COMPONENTS OF THE SBBC

1) PRIVATE PART IN ON-CHAIN OF THE SBBC

Blockchains have difficultly guaranteeing information deletion because all transaction information is distributed to multiple users [18]. Therefore, the proposed on-chain module includes a private part that protects personal information and solves blockchain capacity limitations. The private part issues a license to the consumer to use DRM content and generates the corresponding transaction information as a SB. The consumer creates a smart contract to receive the license, and the content provider subsequently encrypts the secret key that decrypts the encrypted digital content with the consumer's public key and transmits it to the smart contract. The license containing the rules is packaged through the smart contract and transmitted to the consumer. A confirmation message is sent when the consumer successfully receives the license, and the transaction content is generated as a SB. Figure 5 shows the license and SB structure. The license includes a digital content decryption key encrypted with the consumer's public key, along with related rules, including the use time, end time, and duration for the digital content. The hash value for the license is included to ensure license data integrity. The hash value for the previous block, creation time, user authentication information, and content provider information are provided as headers in the SB, and the SB body stores encrypted content and license information [26]. This solves the storage limitations and personal privacy problems because the SB is solely owned by the consumer.

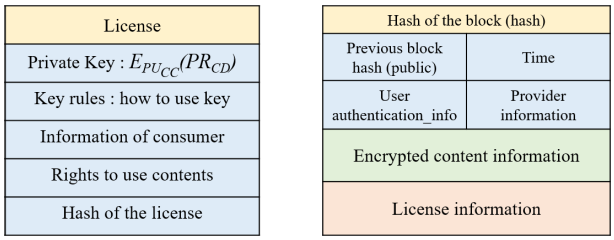


FIGURE 5. License and secret block structure.

2) PUBLIC PART IN ON-CHAIN OF THE SBBC

Private blockchains are operated by the operating entity, and hence malicious action is possible by seizing the operating entity or stealing the authority. To prevent this, the proposed SBBC uses a public blockchain environment, with increased decentralization providing transparency because it is agreed upon by many participants. The on-chain public part includes transaction verification and consensus processes that gather verified transactions and generate blocks. Only the consumer possesses the SB where transaction information is stored for personal information protection. Therefore, transaction verification should also be performed without transaction information. To this end, we employ zero-knowledge proof, that is, proving the user has the information without providing any of that information to the other party. The Schnorr protocol is a representative approach utilizing zero-knowledge proof, providing a mechanism to prove a certifier has the private key without revealing the key, and is widely used for blockchains [27]. The consumer demonstrates they have the license hash value, s, without disclosing s to the blockchain validator. Algorithm 1 and Algorithm 2 show the signature process using the Schnorr protocol, and Figure 6 shows the overall process and includes the proof process. A description of the symbol is given in Table 2. The consumer generates a schnorr signature and sends it to the blockchain network. Verifiers in the blockchain network proceed with the schnorr signature verification.

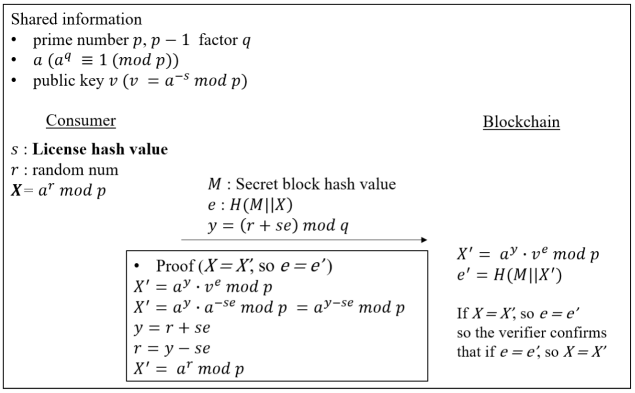


FIGURE 6. Transaction verification using Schnorr protocol.

Algorithm 1 Schnorr Signature Generation

Input: Shared parameters (p, q, a, v), license hash value s, random number r

Output: Signature(e, y)

1: Compute $M = H(SB)$.
2: Compute $X = a^r \bmod p$.
3: Compute $e = H(M||X)$.
4: Compute $y = (r + se) \bmod q$.
5: **return** Signature(e, y)

Transactions that have completed verification are collected in a certain size and timeframe and then generated as blocks. The generated blocks must be validated for all transactions in the public blocks (PBs), and only approved blocks can be chained. The consensus algorithm is used to check block validity. All transactions in the block are determined to be

Algorithm 2 Schnorr Signature Verification

Input: Shared parameters (p, q, a, v), SB hash value M, Signature(e, y)

Output: Acceptance or rejection of the signature

1: Compute $X' = a^y * v^e \bmod p$.
2: Compute $e' = H(M||X')$.
3: If $e = e'$, then return ("Accept the signature")
4: Else, return ("Reject the signature")

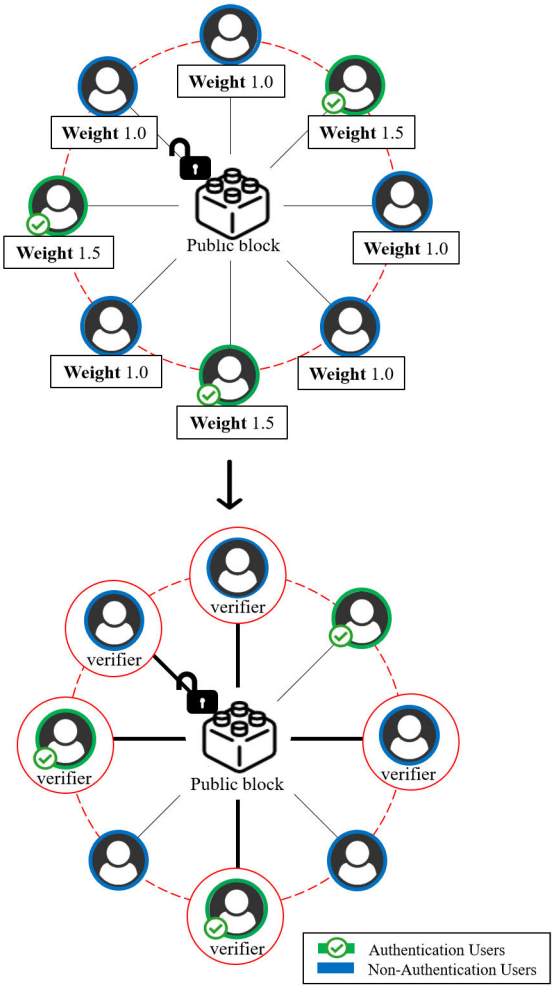


FIGURE 7. Proposed WBFT consensus algorithm.

reliable once consensus is successfully reached. As discussed above, the common PoW and PoS consensus algorithms have problems with energy wastefulness and with the rich getting richer and the poor getting poorer, respectively, along with payment uncertainty and relatively long block creation time. Although the preferred PBFT consensus algorithm solves these performance problems, it has a problem with slower execution time as the number of nodes increases because it considers all consensus participants' intentions, and hence it is unsuitable for public blockchains. The proposed SBBC caters to authenticated and non-authenticated users. Therefore, we propose the WBFT consensus algorithm to address the PBFT problems. WBFT assigns high weights

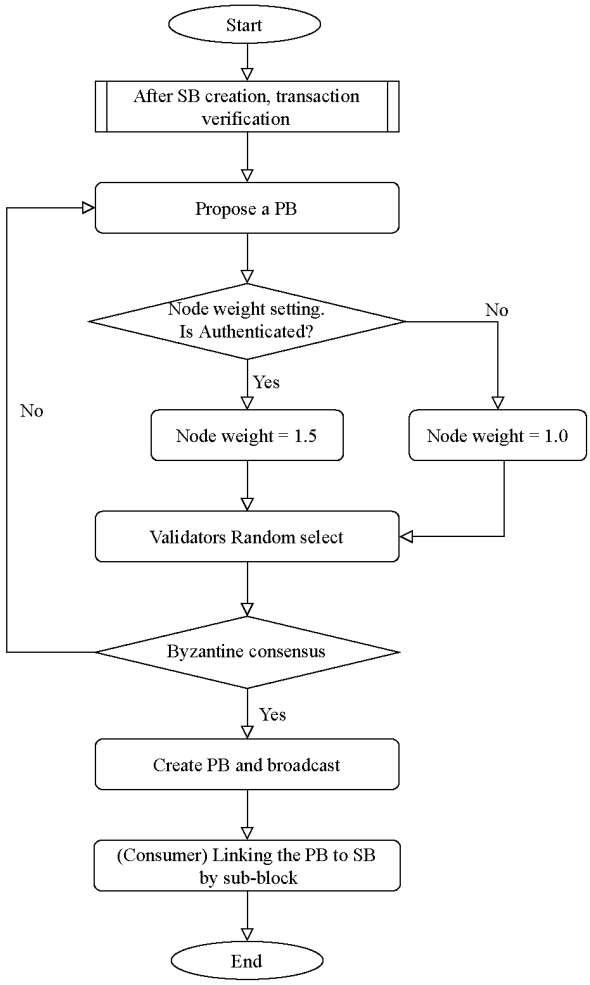


FIGURE 8. Proposed WBFT flow chart.

to authenticated users and randomly selects validators to proceed with consensus. We set the WBFT authenticated user weight = 1.5 and unauthenticated user weight = 1.0. These weights are used for the validator election and agreement result, and consensus reliability is guaranteed because authenticated users are more likely to be elected as the validator. Figure 7 shows that each participant's weight is set depending on whether they are authenticated, and a validator is randomly selected based on those weights. Figure 8 shows the WBFT process as a flow chart.

D. SBBC BLOCK STRUCTURE AND LEDGER STRUCTURE

In addition to improving digital content trading, SBBC comprises a public blockchain, but requires users to be certified to proceed with transactions and smart contracts. This prevents false transactions in the public blockchain and network overload due to the users' validation. WBFT under SBBC allows ledger access because both authenticated and unauthenticated users participate in an agreement that validates transactions and blocks, but only authorized users can access smart contracts. SBs include the previous and current block hash as block headers with encrypted content in the block

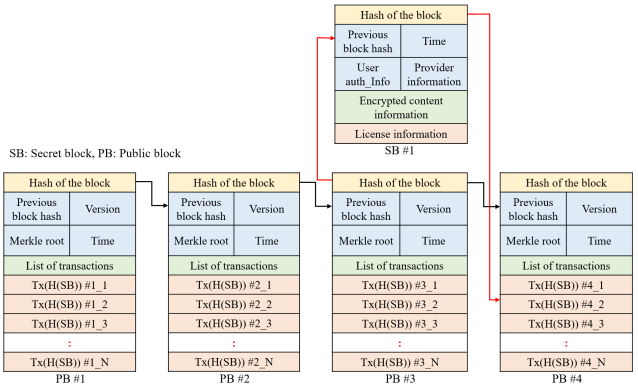


FIGURE 9. Proposed SBBC block connection structure.

body, that is, transaction content and license information to execute the content. Figure 9 shows the proposed SBBC block and connection structure. *SB*#1 is created after *PB*#3 is created, and it stores the *PB*#3 hash value as Previous block hash because *PB*#3 was the last block recorded in the ledger. Thus, *SB*#1 is connected to *PB*#3. Similarly, the *SB*#1 hash value is stored as a transaction in the next block, *PB*#4, connecting *SB*#1 and *PB*#4. Previous block hash in *PB*#4 and *SB*#1 is the *PB*#3 hash. Therefore, the secret block (SB) is a subblock to the public block (PB) with the same hash value as the previous block.

Figure 10 shows the difference in ledger structure among the SBBC participants. SBBC creates a SB owned only by the trading party, meaning that participants have different ledgers. Participant A has blocks SB_A#1 and SB_A#2, with existing transaction contents, and the blocks are connected as subblocks to *PB*#3 and *PB*#5, respectively. Participant B has SB_B#1, which is connected and stored as a subblock to *PB*#4. Thus, it can be said that PB is a structure that all users have in common, and SB is added according to the number of their transactions. Since only the user owns the SB that stores the digital contents, blockchain storage limitations are avoided, and user privacy is also guaranteed.

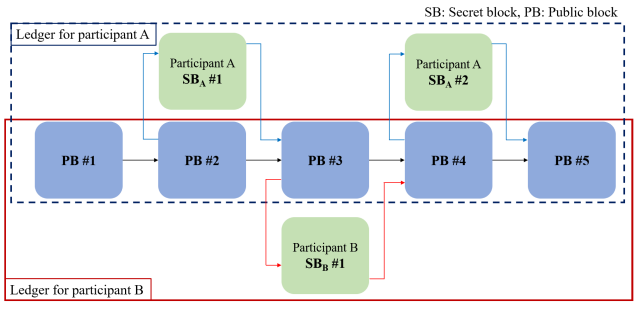


FIGURE 10. Proposed SBBC participant ledger structure.

IV. EVALUATION AND ANALYSIS

For experimentation, we used a virtual machine that was allocated three Intel Core i7-10700 64-bit CPUs @ 2.90 GHz and 48GB RAM, 200GB hard drive space, and running Ubuntu 20.04.2 LTS. We used Hyperledger Sawtooth and Hyperledger Caliper for experiment in the blockchain environment. Hyperledger Sawtooth is the tool that allows you to experiment with PBFT consensus algorithms in a blockchain environment. In addition to PBFT, the Proof of Elapsed Time (PoET) consensus algorithm proposed by Hyperledger Sawtooth can also be tested. Hyperledger Caliper is a tool that can measure blockchain performance. Hyperledger caliper measures the performance by benchmarking the blockchain and provides the results in a report format. The PBFT consensus algorithm uses the open-source version of Hyperledger Sawtooth 1.0, provided by IBM [28]. The blockchain network was connected to the consensus engine and network through a TCP port. Each node of the blockchain network communicated through the Rest-API and executed a transaction processor to proceed with consensus. The test gradually increased the number of nodes and recorded the consensus execution time. The WBFT consensus algorithm also confirmed the consensus algorithm execution time using the open-source Hyperledger Sawtooth 1.0 and compared the outcomes with those of the PBFT algorithm. We also used open-source Hyperledger Caliper 0.3 to analyze the blockchain efficiency [29]. Each blockchain environment using the PBFT and WBFT algorithms was simulated by benchmarking Hyperledger Sawtooth through Hyperledger Caliper.

A. CONSENSUS ALGORITHM COMPLEXITY ANALYSIS

PBFT broadcasts a message for consensus to all nodes participating in consensus and must receive a valid message from at least two-thirds of the nodes. Therefore, when the number of nodes participating in the total consensus is N, the communication complexity of PBFT is $O(N^2)$. T-PBFT, an algorithm that improves PBFT, computes the trust value of each node [23]. A node with a high confidence value by a constant percentage d is then elected, and consensus proceeds. At this time, if the value of $d = 1$, the communication complexity becomes $O(N^2)$ because all nodes participate in consensus. G-PBFT selects a node to proceed with consensus considering the geographic situation of IoT [24]. When the number of nodes participating in the actual consensus is C, G-PBFT fixs the minimum and maximum values of C in the genesis block. Therefore, the communication complexity of G-PBFT becomes $O(C^2)$. When executing proposed WBFT for consensus, users who are authenticated by the verifier pool always exist. This is because consensus occurs after the transaction is made, and the system cannot create a transaction unless it is authenticated. In particular, because consensus on blocks is made by gathering several transactions, there must be at least two authenticated users (the content provider and a consumer). Therefore, the communication complexity of WBFT is $O((N-1)^2)$. Because the weight of an authenticated user is 1.5, the consensus trust of three unauthenticated users is the same as the consensus trust of the two authenticated users. Therefore, when considering the worst case in which all unauthenticated users are selected in a network in which only two authenticated users exist, a reliable

consensus can be derived even if only one authenticated user is selected.

B. COMPARISON OF PBFT AND WBFT CONSENSUS ALGORITHMS

We developed and applied the WBFT algorithm to solve digital content trading problems using the proposed SBBC. The WBFT reaches consensus by applying different weights depending on whether the user is authenticated, with authenticated users being assigned relatively higher weights. If the weight is set too high, only authenticated users can participate in the validation, allowing malicious actions such as collusion and monopoly. Therefore, it is important to set appropriate weights to prevent malicious behavior [30].

$$f_a = \frac{\sum_{i=1}^{n}(k \cdot f(i) + b)}{n} \tag{1}$$

The fairness level (b) was set to 1.0, where all nodes are in a fair state. When the fair state was 1.0, the fairness reduction factor (k) was set to the differences in value from 1.0. $f(i)$ was set as the amount of consensus participation of authenticated nodes. Authenticated and unauthenticated users coexist under SBBC; hence, the simulation gradually increased the proportion of authenticated users. Since it is possible to manipulate block contents when occupying more than 50% of a blockchain network, we set 50% as the threshold value for weight setting according to fairness.

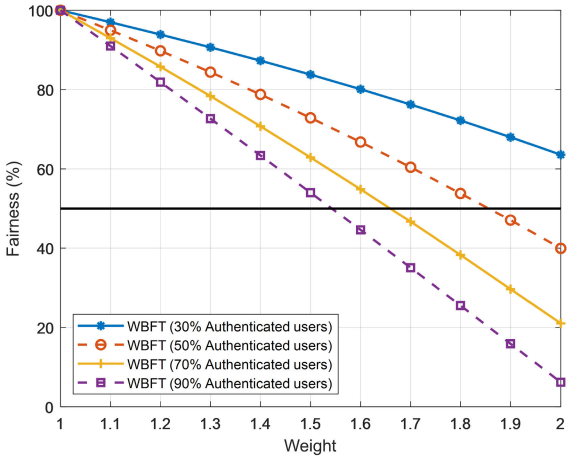


FIGURE 11. Node fairness measurement by weight.

Figure 11 shows the node fairness with respect to the weight, calculated from Eq.(1) for the simulated SBBC. Fairness decreased rapidly for 90% authenticated users, falling below 50% for authenticated weight > 1.5. Therefore, considering the worst case of many authenticated users, we set the authenticated user weight = 1.5. This simulation was conducted by increasing the number of nodes participating in the consensus by five. Figure 12 compares the consensus execution time for PBFT and WBFT with respect to the number of nodes. Although the execution time increased as the number of nodes increased, the WBFT consensus

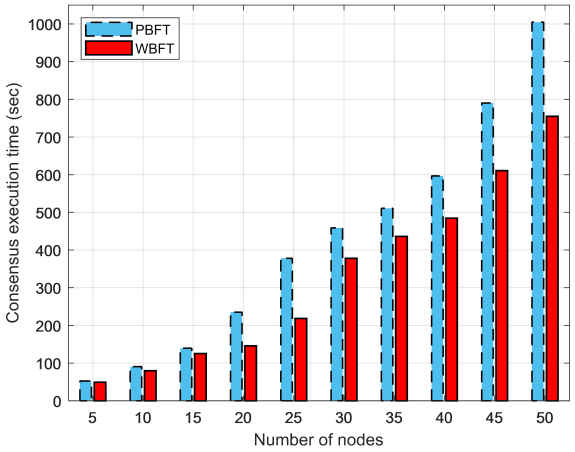


FIGURE 12. PBFT and WBFT consensus execution time.

algorithm took less time on average than the PBFT because WBFT selects fewer nodes than PBFT to proceed with consensus. Figure 13 compares the consensus execution time with respect to the authenticated user proportion in the SBBC. The number of nodes selected for consensus decreases as the authenticated user proportion increases, and thus the consensus execution time decreases. In particular, the consensus execution time when the authenticated user proportion = 70% was approximately 40% better than the current PBFT consensus algorithm.

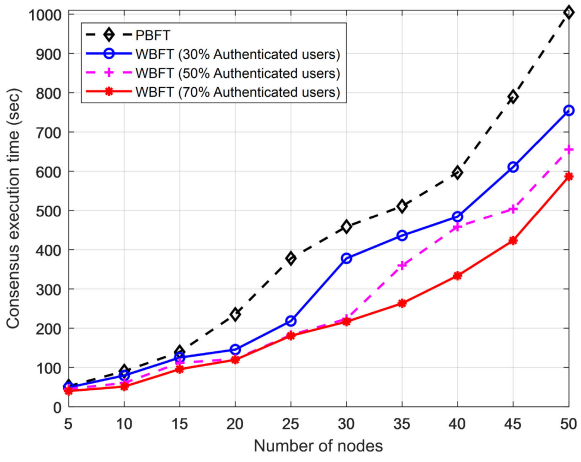


FIGURE 13. WBFT consensus execution time with respect to authenticated user proportion.

C. EFFICIENCY ANALYSIS

Efficiency is a very important factor for network systems. This paper used Hyperledger Caliper to benchmark Hyperledger Sawtooth. The simulation considered network performance for 50 transactions delivered to the blockchain using PBFT and WBFT consensus algorithms at 10 TPS. Figure 14 compares the transaction processing latency for the PBFT and WBFT algorithms. The transaction waiting time increased as the number of nodes increased for

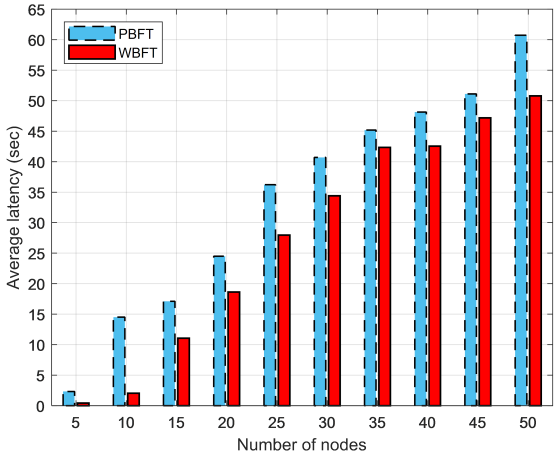


FIGURE 14. Transaction processing latency for blockchain using PBFT and WBFT.

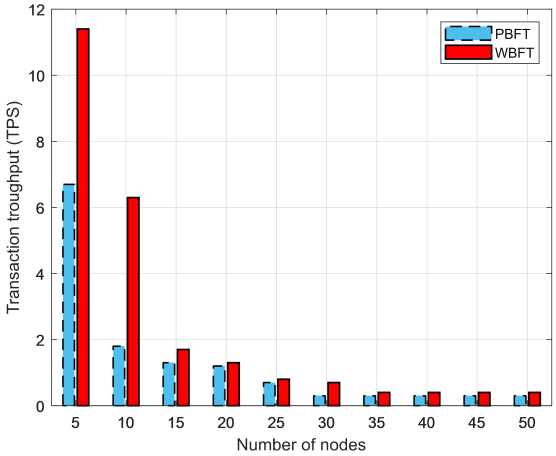


FIGURE 16. Throughput for blockchain using PBFT and WBFT.

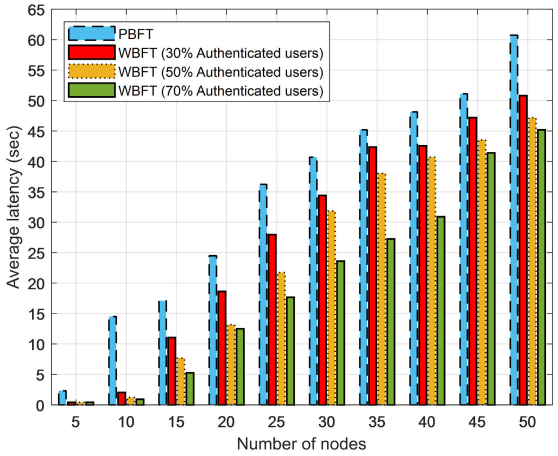


FIGURE 15. WBFT transaction processing latency with respect to authenticated user proportion.

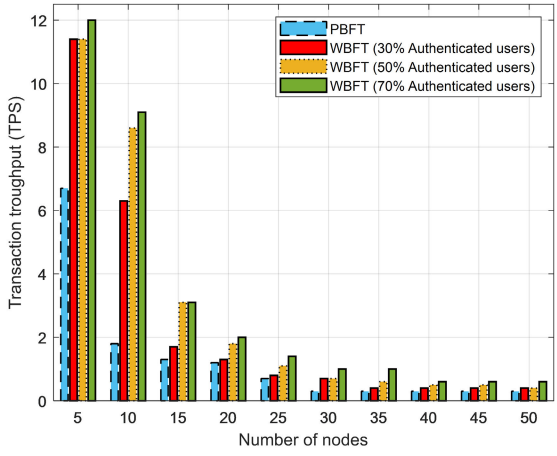


FIGURE 17. WBFT throughput with respect to authenticated user proportion.

both algorithms, but WBFT had shorter latency than PBFT. Figure 15 shows that the transaction wait time shortened as the authenticated user proportion increased. Figures 16 and 17 show that WBFT provided higher throughput than PBFT and that throughput increased with an increasing authenticated user proportion, respectively.

Then, we measured the average validator CPU and memory usage with respect to the number of transactions. Many nodes do not participate in consensus when the number of nodes is too high; hence, it is difficult to produce an objective result to calculate the average resource usage for each node. In the simulation environment, we fixed the parameter at 30 nodes. At this level, all nodes participated in the consensus and produced the most stable result. Verifier resource usage for consensus, namely, CPU and memory, increased as the number of transactions to be processed increased. Figures 17 and 18 show that resource usage increased unevenly as the transaction processing increased. This is because we derived the average validator resource quantities whereas each validator has a different resource performance. Figure 18 shows that the average CPU usage is lower in the blockchain using WBFT than when using PBFT. Figure 19 shows the average validator memory usage as the transaction processing increased. Like CPU usage, more memory was used to handle many transactions. However, the average memory usage was lower for blockchains using WBFT than with those using PBFT, with the difference increasing for increased transactions. The simulations showed that nodes began to fail consensus when the number of transactions exceeded approximately 100, and an objective result could not be derived for average resource usage. Because as more transactions need to be processed, the amount of node communication increases, which eventually leads to traffic overload. Therefore, it was impossible to simulate more than 100 transactions, although we expect memory usage differences for each blockchain to increase when many transactions are processed in real-world applications. Thus, when many users participate in WBFT consensus, increasing authenticated user proportion will increase overall speed and throughput.

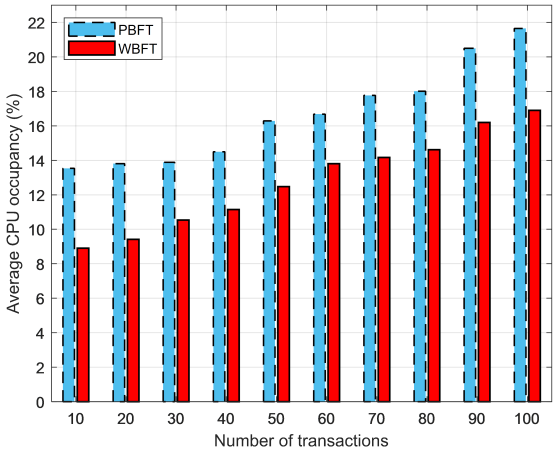


FIGURE 18. Average validator CPU usage with respect to the number of transactions in blockchains using PBFT and WBFT.

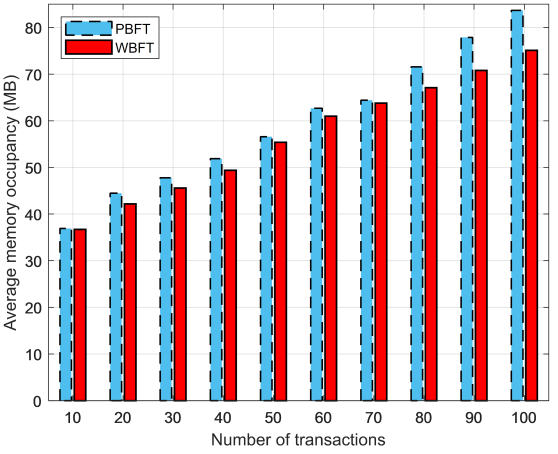


FIGURE 19. Average validator memory usage with respect to the number of transactions in blockchains using PBFT and WBFT.

D. SECURITY ANALYSIS

Information systems must ensure integrity, availability, and confidentiality [31]. Compliance with GDPR regarding protecting personal information is also an important security factor. Integrity is guaranteed in the proposed SBBC because all transactions are created in blocks, stored in a chain, and distributed and recorded such that they cannot be forged or tampered with. The proposed SBBC includes the basic public blockchain structure, guaranteeing transparency and data integrity. However, false transactions can occur in public blockchains because anyone can create and verify transactions. Thus, waiting time to check transaction validity increases, and hence network load increases, reducing availability. SBBC avoids reduced availability by allowing only authorized users to proceed with transactions, and it ensures confidentiality because transaction contents can only be confirmed by the trading party through SBs, hence solving personal information leakage. Because authenticated and unauthenticated users coexist in the proposed SBBC, we propose the WBFT consensus algorithm to increase consensus credibility by ensuring authenticated users preferentially participate in consensus due to their relatively high selection weight. This also improves consensus speed.

Thus, the proposed SBBC creates a secure digital content trading environment, solves blockchain storage limitations when trading large amounts of digital content, and also solves illegal copying and leaking by combining blockchain, DRM, and digital fingerprinting.

V. CONCLUSION

Many digital content types have been developed with the advent of the information age, such as VR, AR, and MR. Digital content market size and consumption have steadily increased, emphasizing digital content importance. However, distributing and sharing digital content through networks gives rise to various problems, such as illegal copying and leaking, profit distribution, forgery, and falsification. Blockchain technology offers new solutions for these problems. This study improved DRM and digital fingerprinting to solve illegal digital content copying and leaking, and it also incorporated blockchain to solve profit distribution, forgery, and falsification problems. However, blockchains have space limitations and cannot store large digital content. Wasted storage space and insufficient privacy protection are also critical because transactions, including their contents, are all distributed and stored in each peer's storage. The proposed SBBC system includes off-chain and on-chain modules to establish secure and reliable digital content trading. We also proposed the WBFT consensus algorithm, which sets consensus weights based on whether users are authenticated, further improving reliability. Consequently, SBBC ensures security and reliability by resolving and grafting current problems that have become critical issues.

The proposed SBBC can be applied not only to digital content trading but also to medical systems, where privacy is important, and logistics systems, where high participation must be balanced with transaction processing speed. However, SBBC is optimized for digital content trading environment. When you extend SBBC to other application areas, some mechanisms which are adopted in this work, such as DRM or digital fingerprints, need to be replaced with other ones. For example, in medical systems, the anonymity of medical data is important, and the mechanisms for anonymity such as differential privacy are much more appropriate than digital fingerprinting. Thus, in our future work, we will develop a reliable and portable blockchain system that can be applied to various environments by improving those aspects.

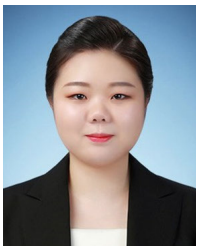
REFERENCES

[1] R. Xu, L. Zhang, H. Zhao, and Y. peng, "Design of network media's digital rights management scheme based on blockchain technology," in *Proc. IEEE Int. Symp. Auton. Decentralized Syst. (ISADS)*, Mar. 2017, pp. 128–133.

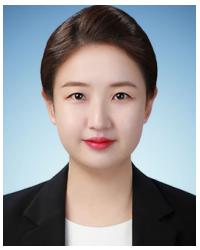
[2] A. Savelyev, "Copyright in the blockchain era: Promises and challenges," *Comput. Law Secur. Rev.*, vol. 34, no. 3, pp. 550–561, Jun. 2018.

[3] S. Lian, D. Kanellopoulos, and G. Ruffo, "Recent advances in multimedia information system security," *Informatica*, vol. 33, no. 1, pp. 3–24, Mar. 2009.

[4] M. Holland, C. Nigischer, J. Stjepandić, and C. Chen, "Copyright protection in additive manufacturing with blockchain approach," *Transdisciplinary Eng., A Paradigm Shift*, vol. 5, pp. 914–921, Jul. 2017.
[5] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, "A survey on privacy protection in blockchain system," *J. Netw. Comput. Appl.*, vol. 126, pp. 45–58, Jan. 2019.
[6] G. Heo, D. Yang, I. Doh, and K. Chae, "Design of blockchain system for protection of personal information in digital content trading environment," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Jan. 2020, pp. 152–157.
[7] U. Khan, Z. Y. An, and A. Imran, "A blockchain ethereum technology-enabled digital content: Development of trading and sharing economy data," *IEEE Access*, vol. 8, pp. 217045–217056, Nov. 2020.
[8] A. Piva, F. Bartolini, and M. Barni, "Managing copyright in open networks," *IEEE Internet Comput.*, vol. 6, no. 3, pp. 18–26, May 2002.
[9] M. Campidoglio, F. Frattolillo, and F. Landolfi, "The copyright protection problem: Challenges and suggestions," in *Proc. 4th Int. Conf. Internet Web Appl. Services*, 2009, pp. 522–526.
[10] J. Berti, "Copyright infringement and protection in the Internet age," *IT Prof.*, vol. 11, no. 6, pp. 42–45, Nov. 2009.
[11] Z. Ma, M. Jiang, H. Gao, and Z. Wang, "Blockchain for digital rights management," *Future Gener. Comput. Syst.*, vol. 89, pp. 746–764, Dec. 2018.
[12] Q. Liu, R. Safavi-Naini, and N. P. Sheppard, "Digital rights management for content distribution," in *Proc. Australas. Inf. Secur. Workshop Conf. ACSW Frontiers*, vol. 21, Jan. 2003, pp. 49–58.
[13] I. J. Cox, M. L. Miller, J. A. Bloom, and C. Honsinger, *Digital Watermarking*, vol. 53. San Francisco, CA, USA: Morgan Kaufmann, 2002.
[14] S. Rouhani and R. Deters, "Security, performance, and applications of smart contracts: A systematic survey," *IEEE Access*, vol. 7, pp. 50759–50779, Apr. 2019.
[15] W. Hon, J. Palfreyman, and M. Tegart, "Distributed ledger technology & cybersecurity–Improving information security in the financial sector," in *Proc. Eur. Union Agency Netw. Inf. Secur. (ENISA)*, Dec. 2016, pp. 1–36.
[16] L. Kan, Y. Wei, A. Hafiz Muhammad, W. Siyuan, L. C. Gao, and H. Kai, "A multiple blockchains architecture on inter-blockchain communication," in *Proc. IEEE Int. Conf. Softw. Qual., Rel. Secur. Companion (QRS-C)*, Jul. 2018, pp. 139–145.
[17] K. Bhaskaran, P. Ilfrich, D. Liffman, C. Vecchiola, P. Jayachandran, A. Kumar, F. Lim, K. Nandakumar, Z. Qin, V. Ramakrishna, E. G. Teo, and C. H. Suen, "Double-blind consent-driven data sharing on blockchain," in *Proc. IEEE Int. Conf. Cloud Eng. (IC2E)*, Apr. 2018, pp. 385–391.
[18] C. Wirth and M. Kolain, "Privacy by blockchain design: A blockchain-enabled GDPR-compliant approach for handling personal data," in *Proc. ERCIM Blockchain Workshop, Eur. Soc. Socially Embedded Technol. (EUSSET)*, 2018, pp. 1–7.
[19] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, "A survey on consensus mechanisms and mining strategy management in blockchain networks," *IEEE Access*, vol. 7, pp. 22328–22370, Jan. 2019.
[20] S. Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Accessed: Nov. 1, 2020. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[21] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, "Everything you wanted to know about the blockchain: Its promise, components, processes, and problems," *IEEE Consum. Electron. Mag.*, vol. 7, no. 4, pp. 6–14, Jul. 2018.
[22] Y. Hao, Y. Li, X. Dong, L. Fang, and P. Chen, "Performance analysis of consensus algorithm in private blockchain," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Jun. 2018, pp. 280–285.
[23] S. Gao, T. Yu, J. Zhu, and W. Cai, "T-PBFT: An EigenTrust-based practical byzantine fault tolerance consensus algorithm," *China Commun.*, vol. 16, no. 12, pp. 111–123, Dec. 2019.
[24] L. Lao, X. Dai, B. Xiao, and S. Guo, "G-PBFT: A location-based and scalable consensus protocol for IoT-blockchain applications," in *Proc. IEEE Int. Parallel Distrib. Process. Symp. (IPDPS)*, May 2020, pp. 664–673.
[25] Z. Meng, T. Morizumi, S. Miyata, and H. Kinoshita, "Design scheme of copyright management system based on digital watermarking and blockchain," in *Proc. IEEE 42nd Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, Jul. 2018, pp. 359–364.
[26] Z. Zhang and L. Zhao, "A design of digital rights management mechanism based on blockchain technology," in *Proc. Int. Conf. Blockchain*, Jun. 2018, pp. 32–46.
[27] J. Camenisch, A. Kiayias, and M. Yung, "On the portability of generalized schnorr proofs," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, 2009, pp. 425–442.
[28] *Hyperledger Sawtooth-PBFT*. Accessed: Dec. 1, 2020. [Online]. Available: https://sawtooth.hyperledger.org/docs/pbft/releases/1.0.0/
[29] N. Lincoln, *A blockchain Perform. benchmark framework Hyperledger Caliper*. Accessed: Feb. 1, 2021. [Online]. Available: https://hyperledger.github.io/caliper/
[30] N. D. Tam, "A decision-making phase-space model for fairness assessment," *Psychol. Behav. Sci.*, vol. 3, nos. 1–6, pp. 8–15, Jan. 2014.
[31] D. Coss, "The cia strikes back: Redefining confidentiality, integrity and availability in security," *J. Inf. Syst. Secur.*, vol. 10, no. 3, pp. 21–45, Jul. 2014.



GABIN HEO received the B.S. degree from the Department of Cyber Security, Kyungil University, in 2018, and the M.S. degree in computer science and engineering from Ewha Womans University, Seoul, South Korea, in 2020, where she is currently pursuing the Ph.D. degree with the Division of Artificial Intelligence and Software. Her research interests include blockchain, authentication, digital content security, and the IoT security.



DANA YANG received the B.S. degree from the Department of Computer Software, Korean Bible University, in 2013. She is currently pursuing the Ph.D. degree with the Department of Computer Science and Engineering, Ewha Womans University, Seoul, South Korea. Her research interests include authentication, blockchain, steganography, flying adhoc network (FANET) security, and D2D network security. She received the Outstanding Paper Award from the 20th International Conference on Advanced Communication Technology (ICACT), in 2018.

INSHIL DOH received the B.S. and M.S. degrees in computer science, and the Ph.D. degree in computer science and engineering from Ewha Womans University, Seoul, South Korea, in 1993, 1995, and 2007, respectively. From 1995 to 1998, she worked with Samsung SDS, South Korea. She was a Research Professor with Ewha Womans University, from 2009 to 2010, and Sungkyunkwan University, in 2011. She is currently an Associate Professor with the Department of Cyber Security, Ewha Womans University. Her research interests include wireless network security, sensor network security, and the IoT network security.

KIJOON CHAE received the B.S. degree in mathematics from Yonsei University, in 1982, the M.S. degree in computer science from Syracuse University, in 1984, and the Ph.D. degree in electrical and computer engineering from North Carolina State University, in 1990. He is currently a Professor with the Department of Computer Science and Engineering, Ewha Womans University, Seoul, South Korea. His research interests include blockchain, security of flying ad hoc networks (FANET), sensor networks, smart grid, CDN, SDN, the IoT, network protocol design, and performance evaluation.