International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 9-No.4 (2023) pp. 419-434
http://dergipark.org.tr/en/pub/ijcesen

ISSN: 2149-9144

Research Article

OTA 2.0: An Advanced and Secure Blockchain Steganography Algorithm

Mustafa TAKAOĞLU[1*], Adem ÖZYAVAŞ[2], Naim AJLOUNİ[3], Taner DURSUN[4], Faruk TAKAOĞLU[5], Selin DEMİR[6]

[1]TÜBİTAK, BİLGEM, UEKAE, Department of Blockchain Technologies (BZLAB), 41400, Kocaeli-Türkiye
*** Corresponding Author** : **Email:** mustafa.takaoglu@tubitak.gov.tr - **ORCID:** 0000-0002-1634-2705

[2]İstanbul Atlas University, Faculty of Engineering and Natural Sciences, 34413, İstanbul-Türkiye
Email: adem.ozyavas@atlas.edu.tr - **ORCID:** 0000-0001-5375-1826

[3]İstanbul Atlas University, Faculty of Engineering and Natural Sciences, 34413, İstanbul-Türkiye
Email: naim.ajlouni@atlas.edu.tr - **ORCID:** 0000-0002-5116-8933

[4]TÜBİTAK, BİLGEM, UEKAE, Department of Blockchain Technologies (BZLAB), 41400, Kocaeli-Türkiye
Email: taner.dursun@tubitak.gov.tr - **ORCID:** 0000-0001-5893-8219

[5] TÜBİTAK, BİLGEM, UEKAE, Department of Quantum Technologies, 41400, Kocaeli-Türkiye
Email: faruk.takaoglu@tubitak.gov.tr - **ORCID:** 0000-0003-0828-2017

[6]TÜBİTAK, BİLGEM, UEKAE, Department of Blockchain Technologies (BZLAB), 41400, Kocaeli-Türkiye
Email: selin.demir@tubitak.gov.tr - **ORCID:** 0009-0006-6331-6418

Article Info:

DOI: 10.22399/ijcesen.1345417
Received : 18 August 2023
Accepted : 15 December 2023

Keywords

Blockchain Technology
Digital Steganography
Blockchain Steganography
Hyperledger Fabric
Vernam Cipher

Abstract:

Blockchain technology, a disruptive force beyond Bitcoin, is finding applications across various fields, including scientific disciplines like steganography – the art of data hiding. Digital steganography has gained momentum with data digitization, especially in multimedia environments like images, text, audio, and videos. Blockchain's integration into steganography has led to interesting developments, like the OTA (Ozyavas-Takaoglu-Ajlouni) algorithm introduced in 2021. The OTA algorithm consists of two stages: the OTA-steganography algorithm and the OTA-chain algorithm (private blockchain). Developed using Java and JavaScript, the OTA platform utilises OTA-coins as its native currency. Previous versions allowed various file types as cover-multimedia, with the secret message encrypted using the Vernam Cipher symmetric encryption and hidden using OTA steganography. Unlike other steganography methods, OTA doesn't alter the cover-multimedia but uses bit-level data marking. In the OTA system, the marked data indices are stored in 1 KB arrays and transmitted to the receiver as transactions via OTA-chain, each incurring a fixed fee of 1 OTA-coin to prevent DDoS attacks. The OTA 2.0 algorithm improved on the previous version by switching to Hyperledger Fabric protocol, which offers open-source, permissioned blockchain solutions, decentralisation capabilities, and self-sovereign identity support. The new version also enhanced block creation time to 2 seconds, increased block size to 90 MB, and employed a 4-bit marking pattern while eliminating transaction fees. Thanks to its innovative key-sharing method and permissioned architecture, OTA 2.0 proves resistant to steganalysis methods commonly used in steganography studies.

1. Introduction

The confidentiality of information and its secure transmission between parties has been one of the most important topics of study throughout history. The art of data hiding, called steganography, is a very old subject of study. The science of steganography, the first examples of which were seen in the "Didim-Aydın" region of Turkey, has taken a digital form as a result of the emergence of computers and the digitalization of data. Today, data that is desired to be hidden for many different

purposes is shared between the parties by using steganography techniques. The most important basic rule in steganography is not to be noticed. For this reason, steganography is being attempted on many new mediums. Blockchain technology is one of the prominent innovations in this context [1-4].

To put it simply, blockchain technology is a secure, decentralised, and distributed database that stores digital transaction histories. It is based on cryptography and computer science principles. The first example of blockchain technology, which is believed to have started with Bitcoin, dates back to the 1990s, when cryptographers Stuart Haber and W Scott Stornetta introduced the concept of a chain of cryptographically secure blocks [5]. However, there were other attempts before Bitcoin with similar features, such as Digicash, Bitgold, Napster, Gnutella, BitTorrent, Hashcash, and B-money [6-12]. The success of Bitcoin can be attributed to factors like the announcement of its whitepaper [13] in 2008 and global events like economic crises and pandemics that followed. Although the Bitcoin protocol has been successful and contributed to the development of blockchain technology and distributed ledger technology on a broader scale, its single-purpose architecture as a payment system limits its realistic usability in other areas. As a result, the Ethereum protocol introduced the ability to develop smart contracts and the concept of the world state machine (Ethereum-Virtual-Machine, EVM), which paved the way for blockchain technology to be used in various fields [14]. Subsequently, other layer 0 and layer 1 protocols (Solana, Cosmos, Avalanche, Aptos, Algorand, etc.) proposed after Ethereum have provided capabilities for developing smart contracts while attempting to address scalability and interoperability challenges through different approaches [15-19].

In steganography research, the idea of using blockchain protocols or blockchain-based solutions as a medium is one of the explored topics. Suggestions have been made to perform steganography on transaction records or during the mining processes of existing permissionless blockchain protocols [20]. Traditional digital image steganography studies have been conducted using Non-Fungible Tokens (NFTs) and generative art [21]. Additionally, steganalysis methods have been applied to public blockchain transaction records to detect stego-multimedia. Another approach that led to the preparation of this study is the innovative concept known as "Blockchain Steganography," which proposes performing steganography in a blockchain environment. The OTA algorithm introduced in the article titled "A Novel and Robust Hybrid Blockchain and Steganography Scheme" offers a solution using a private blockchain for steganography, rendering existing steganalysis methods ineffective and solving the hiding capacity problem with a unique data hiding method. The study describes an older protocol version called OTA 1.0, which has identified areas open to various improvements since its proposal in 2021, along with the advancement of capabilities in blockchain technology [20]. With the introduction of OTA 2.0, the new method addresses the identified shortcomings and proposes an innovative solution to enhance system security through the distribution of the One-Time-Pad (OTP), a.k.a. Vernam Cipher, symmetric encryption algorithm's key.

In the ongoing sections of the study, a literature review has been shared. The Preliminaries section covers steganography, blockchain technology, Hyperledger Fabric (HLF) blockchain protocol, InterPlanetary File System, OTP symmetric encryption algorithm (Vernam cipher), and the OTA 1.0 method. In the OTA 2.0 section, the proposed method is introduced. The Discussions section includes evaluations and comparisons. In the Conclusion section, the prominent aspects of the proposed method are examined, and the study's findings are discussed.

1.1 Literature Review

Chaudhary et al. [22] explored the combination of machine learning with Blockchain for secure and decentralised transactions. The integration of machine learning addresses constraints and enhances the potential of Blockchain. The study focused on using machine learning in Blockchain to develop a stego cryptography system for secure data communication. With the rapid growth of information and communication technology, communication systems face challenges in security, privacy, service delivery, and network management due to data volume and diverse endpoints. The proposed stego cryptography system offers a solution to achieve decentralised, secure, intelligent, and efficient network operation.

Torki et al. [23] discuss the advantages of using blockchain in steganography, combining its benefits for covert communication and data transmission. They review previous steganography schemes in blockchain, identifying their drawbacks. The authors propose two algorithms for steganography in blockchain: one with high capacity for key and steganography algorithm exchange, and the other with medium capacity for embedding hidden data. Their method is versatile and applicable to popular blockchains like Bitcoin and Ethereum. Experimental results demonstrate the efficiency and practicality of the proposed method in terms of execution time, latency, and steganography fee. The

paper also outlines the challenges of steganography in blockchain from both steganographers' and steganalyzers' perspectives.

Chaudhary et al. [24] introduced a comprehensive approach to enhance data security during communication over the network. Their study proposes utilising Blockchain, Deep Learning, and innovative steganography techniques. They employ hash functions to hide secret data, resulting in high embedding capacity and high-quality data input images. The combination of stego images, hash function-generated datasets, and Blockchain technology enhances data security efficiency. Deep learning algorithms are employed to further strengthen data security in the Blockchain, ensuring no null or duplicate values.

Jahavi et al [25]. proposed a model that uses steganography with neural networks, encryption, and hash functions to hide user identity information within images. These images are then stored on the Ethereum blockchain as NFTs, creating a secure and tamper-proof way to authenticate user identity across multiple platforms.

Sarkar et al. [26] proposed the Stego-chain method, combining Robert's edge detection for increased image embedding payload. Steganography was followed by AES encryption and blockchain transmission in small frames. Receiver retraces the steps with the key to recover information. However, details on blockchain transaction confirmation and reliability logic are lacking, and the study's blockchain content is insufficient.

Mohsin et al. [27] proposed modifications to the Particle Swarm Optimization (PSO) algorithm for secure transmission of COVID-19 data using blockchain. Multiple cover-images were used, and optimal storage locations were identified for each image. Hash values were added to stego-images for integrity. The blockchain system ensures tamper-proofing of stego-images with increased complexity. However, the information shared in the Claims and Limitations sections lacks accuracy and credibility.

Li and Kar [28] propose "B-Spot," a Steganography and Blockchain based photo transmission mechanism. It hides a secret photo within a cover photo using a 3-3-2 LSB image steganography algorithm. The stego-image is divided into blocks and connected by hash values to form a tamper-evident blockchain. A copy of the blockchain is stored in a hash table for recovery. The receiver verifies the blockchain's integrity and recovers lost or tampered blocks using the hash table. The mechanism demonstrates high data capacity, improved imperceptibility, reasonable computing time, and robustness to noise, adding an extra layer of security and robustness to existing schemes.

Basuki and Rosiyadi [29] developed a secure data transmission system using transaction steganography and image steganography methods. The traditional image steganography involved encrypting confidential data using the Ethereum system, creating information like partition number, image URL, and access time. Transaction steganography comprised three stages: transaction field selection, embedding method, and parsing method. Their unique work exemplifies blockchain steganography. The authors thoroughly examined steganography and blockchain systems and successfully applied them in their proposed system.

In the proposed research, Kandasamy and Ajay [30] advocate for the use of Blockchain technology in healthcare to securely exchange user data among hospitals, diagnostic laboratories, and pharmaceutical enterprises. Image-based diagnostics in the health sector are crucial, but securing medical images over public networks raises challenges in confidentiality and integrity. To address this, the researchers utilise steganography as a major tool to improve data security. They propose a system with two layers of security using the LSB (Least Significant Bit) method and encryption to insert medical images into cover images, creating stego images. The entire process is implemented using the MATLAB 2021 version, and simulation results demonstrate the effectiveness of the approach with a minimum mean square error of 0.5 for the extracted images.

Partala [31] proposed a robust system combining blockchain and Least Significant Bit (LSB) in cover communication. This system allows the sender to transmit information through a series of transactions, hiding 1 bit of data in each transaction. The blockchain system was well-designed, and steganography was successfully achieved. The only weakness lies in the time it takes to send data, as it requires more than an hour to transmit approximately 1 byte of data. Additionally, using one transaction for each bit can result in a high number of transactions for large data.

Horng et al. [32] used the RDHEI method with block permutation to encode cover images. They encrypted patient data using the histogram shifting method and concealed it within the cover image. The system operates on the blockchain, ensuring secure data transmission with an embedding rate of 0.8 bits per pixel (bpp). In environments like hospitals with a large amount of patient data, the hidden images have high resolution. However, for large datasets, the blockchain system, encryption processes, and steganography steps in this proposed system may take a long time to operate.

Xu et al. [33] proposed a steganography study utilising a method developed over public blockchain

transactions. It involves creating a new block by manipulating selected transactions and embedding steganographic information within it. However, the applicability of this method raises concerns because in many public blockchain systems, miners require significant processing power to create blocks.

Mazdutt et al. [34] discovered 1600 irregular transaction records in the Bitcoin Blockchain, which were different from the system-generated data. These entries can be easily identified, and efforts are ongoing to prevent such data anomalies. However, Xu et al. did not specify how to embed the stego-data they created into the block structure of a public blockchain without detection.

Giron et al. [35] proposed a steganalysis method to detect steganography techniques on the blockchain system. Despite their extensive research, they did not find any evidence of steganography on public blockchain systems. However, they observed some misuse of steganography in the suggested blockchain steganography studies in the literature. They applied Sequential analysis and Clustering analysis steganalysis methods on a large dataset consisting of Bitcoin and Ethereum blocks and bitcoin clusters. The study indicated that further work is needed in this area.

2. Prelimerities

In the Preliminaries section of this article, an in-depth exploration of essential concepts and technologies is undertaken to provide a solid foundation for subsequent discussions. The first subject of investigation is steganography, a discreet information transmission technique that conceals data within seemingly benign cover media, such as images, text, video or audio files. In the blockchain part of the article investigates the revolutionary domain of blockchain technology. This transformative innovation has disrupted diverse industries, enabling decentralised, secure, and tamper-resistant data storage and transactions. Specifically, the focus lies on the Hyperledger Fabric (HLF) blockchain protocol, distinguished for its permissioned and modular architecture, rendering it highly suited for enterprise blockchain applications. In addition, the examination extends to the InterPlanetary File System (IPFS), a peer-to-peer distributed file system offering an innovative approach to data storage and retrieval, ensuring content availability and resilience. Furthermore, the study delves into the OTP symmetric encryption algorithm, renowned for its exceptional security attributes. Based on the concept of a one-time pad, this algorithm achieves encryption and decryption of information, effectively precluding any potential cryptanalysis. Finally, a comprehensive explanation of the OTA 1.0 blockchain steganography method is presented in this article.

2.1 Steganography

The term "steganography" is derived from the Greek words "steganos," meaning hidden, and "graphia," meaning writing. Steganography, an ancient subject of study, initially presented its early examples using physical techniques. Nowadays, with the transformation of information into data, steganography techniques are conducted in the computer environment and referred to as digital steganography. In a broader context, various techniques are employed to safeguard information/data from unauthorised parties, and these efforts are termed "information security." Information security encompasses two main aspects: cryptography and information hiding. Information hiding includes two subcategories: digital watermarking and digital steganography. Digital steganography further divides into linguistic and technical approaches [1-4].

Technical steganography is performed using various chosen methods on different covers such as images, text, videos, audios, and protocols. Among the methods, the most suitable one is selected for the specific cover. The selection is based on spatial domain and frequency domain techniques. Spatial domain methods involve the direct encoding of messages within pixel intensities, whereas transform domain techniques, also referred to as frequency domain images, entail a two-step process: transformation followed by message embedding within the image. Figure 1 presents the taxonomy of steganography [36].

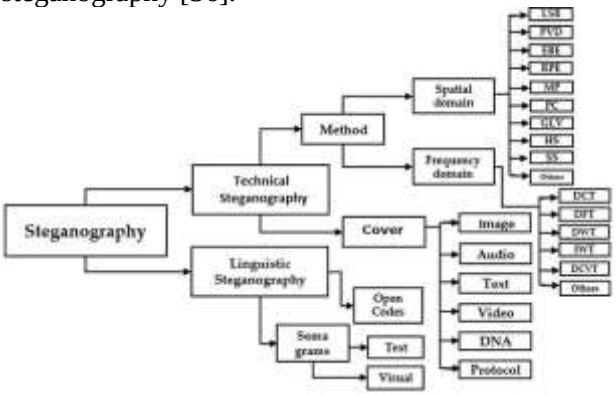

Figure 1. *Taxonomy of steganography [36].*

The application of the Least-Significant-Bit is an uncomplicated and rapid steganography method. To illustrate this in the context of an image cover, the process involves modifying the last 1 or 2 bits of each byte within the cover-image file at the byte level, resulting in a concealment operation. The visual outcome obtained by applying LSB to the

original image (cover-image), thereby hiding data, is termed the stego-image. Figure 2 depicts a visual representation explaining the 2-bit LSB technique applied to the utilised image [37].

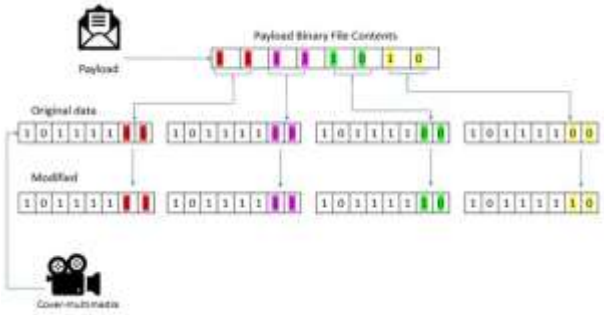

Figure 2. *Least Significant Bit (2-Bit) [37].*

However, the LSB technique introduces visual distortions on the cover-image as changes are made on a bit-level, and these distortions can be detected using steganalysis methods. In the OTA 1.0 study, the proposed OTA-Steganography technique achieves data concealment on the cover-image at the bit level, similar to the LSB technique, but with a difference: instead of altering, it marks, ensuring data hiding without causing any modifications to the cover-image. During the marking process, the indices of matching bits are stored in arrays and are present on the blockchain. The utilised OTA-steganography method enables the concealment (marking) of vast amounts of information on the chosen cover-image without the concern of hiding capacity limitations. The goal of maintaining a high Peak-Signal-to-Noise Ratio (PSNR) value, indicating no alterations on the cover-image, is also achieved. Furthermore, the feasibility of steganalysis methods like Histogram analysis is eliminated [20].

2.2 Blockchain Technology

In 2008, an individual or organisation using the pseudonym Satoshi Nakamoto introduced Bitcoin, a decentralised, distributed, secure, and transparent solution that eliminates intermediaries, in the whitepaper titled "Bitcoin: A Peer-to-Peer Electronic Cash System." In the Bitcoin protocol, system security is ensured not through any encryption algorithm but solely through hash (Sha256) and the Elliptic Curve Digital Signature Algorithm (ECDSA). The Bitcoin protocol, developed in a public structure, allows anyone to participate as a miner, node, or user at any desired time and to exit as well. The system is fault-tolerant and remains unaffected by such developments. The protocol employs a proof-of-work (PoW) consensus algorithm, where miners solving a mathematical puzzle earn the right to create a block and produce a new block. Additionally, the inclusion of currency into the system is carried out by miners within the protocol. However, a notable weakness of the Bitcoin protocol is its requirement for high computational power in the mining process, leading to substantial energy consumption. Another weakness lies in the relatively low transaction rate of 3-7 transactions per second (with a block creation time of 10 minutes). The monolithic nature of the Bitcoin protocol, developed solely as a payment system, has hindered its potential use in various technological domains. Despite recent efforts to develop Non-Fungible Tokens (NFTs) on the Bitcoin protocol, through solutions like Bitcoin Ordinals, it remains challenging to achieve universal applicability across all fields [13,21]. The architectural representation of the Bitcoin protocol is shared in Figure 3 [38].

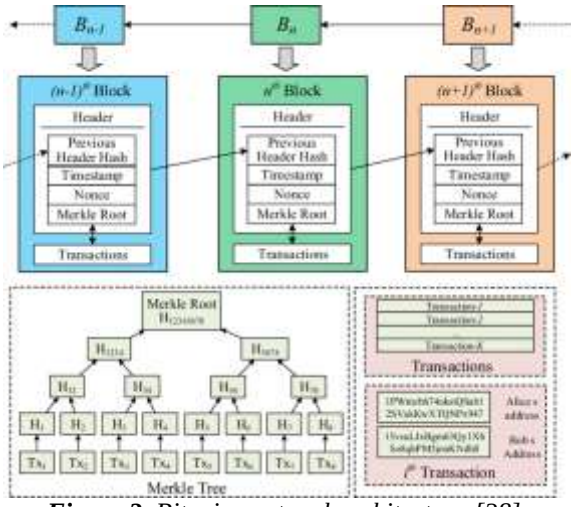

Figure 3. *Bitcoin protocol architecture [38].*

The solution that emerged with the Ethereum protocol, proposed by Vitalik, has paved the way for the broader applicability of blockchain technology beyond the prominent payment systems of the Bitcoin protocol. The Ethereum protocol, introduced with its world state machine concept, Ethereum Virtual Machine, and smart contract features, has facilitated the decentralised, non-centralized, secure, and immutable nature of blockchain technology to be applied across various domains. Until the Merge fork that occurred on September 15, 2022, the Ethereum protocol utilised the Proof-of-Work (PoW) consensus algorithm, transitioning to Proof-of-Stake (PoS) after the Merge. Post-Merge, the Ethereum protocol has transformed into a Layer 1 blockchain protocol with significantly reduced energy consumption. However, similar to Bitcoin, the Ethereum protocol's transaction rate per second is not very high (between 14-110). Layer 2 architectures are being developed to address scalability issues in the Ethereum protocol. Yet,

future forks will play a significant role in introducing the high transaction capabilities seen in protocols like Solana to the Ethereum protocol. The concept of smart contracts, initially introduced with the Ethereum protocol, has opened the door for the applicability of blockchain technology in various fields. Smart contracts, developed to fulfil requirements in projects, execute on the Ethereum Virtual Machine (EVM). Users interacting with smart contracts pay transaction costs, and afterward, predefined conditions within the smart contract are triggered. Applications developed through smart contracts on the EVM are referred to as decentralised applications (DApps) [14].

The capability to develop smart contracts is not exclusive to the Ethereum protocol; nowadays, it is possible to develop smart contracts on various Layer 0 and Layer 1 protocols. Specifically, within Ethereum, smart contracts are developed using programming languages such as Solidity or Viper. In the Hyperledger Fabric (HLF) protocol, smart contracts are referred to as "chaincode," and in the Solana protocol, they are referred to as "programs." The ability to develop smart contracts also enables token creation, allowing for the tokenization of various assets today. Another significant advancement is the development of Decentralised Autonomous Organizations (DAOs) through smart contracts. For instance, utilising numerous smart contracts, it becomes feasible to autonomously and decentralise the entire range of services provided by an entity like a Notary Office on the blockchain network [14,15,39]. One of the innovations brought about by blockchain technology is the concept of new-generation digital identities and digital identity management systems. The concept of Decentralised Identifiers (DIDs) was standardised by the World Wide Web Consortium (W3C) in 2022. Verified identity information produced by an authorised Issuer (usually a government) is provided to users (Holders), and Verifiers can rapidly verify whether the Holder's possessed verifiable credential (VC) is accurate or not through the blockchain network. Thanks to this innovation, all competencies and credentials individuals possess and need to verify can become cryptographically shareable with counterparties without revealing sensitive information or with limited (selective disclosure) sharing. These and similar capabilities make blockchain technology one of the most applicable and effective alternatives in various fields today [40]. Protocols like Bitcoin, Ethereum, and Solana are entirely open to user access, known as permissionless solutions. In developed projects, it might be necessary to restrict system access and define interaction permissions, including write and read rights, at different levels for users in alignment with specified requirements. In this context, permissioned blockchain protocols are used, which are favoured in the digital transformation projects of numerous private sector companies and public institutions. Both permissionless and permissioned blockchain protocols are almost entirely open source and are supported by the community [40].

2.3 Hyperledger Fabric Protocol

Hyperledger Fabric (HLF) protocol is a project within the Hyperledger Foundation family that is utilised in permissioned blockchain projects. HLF, an open-source blockchain protocol, is being developed by a community of developers. Presently, there are numerous software projects developed using HLF. The reason for HLF's widespread adoption can be attributed to its modular structure. Thanks to its modular design, various capabilities like consensus and membership services, decentralised identity plugins (Decentralised Identifiers), Hardware Security Module (HSM) integrations, and more can be added or removed from projects. The concept and capability of smart contracts introduced in the Ethereum protocol are presented in the HLF protocol as chaincode. HLF follows a container approach. Furthermore, transaction privacy, introduced as channels, ensures that only authorised nodes of a particular channel can access transactions. While the HLF protocol might not exhibit very high transaction per second (TPS) rates, its performance varies depending on the project's requirements, architecture, and complexity. Additionally, in HLF, the Membership Service Provider (MSP) specifies the rules for validating, authenticating identities, and granting access to the blockchain network. In HLF, clients initiate the creation of transactions. Within HLF, there are two types of peers: endorsing and committing peers. Peers are involved in the execution of chaincode. Furthermore, in the protocol, Orderer nodes play a role in achieving consensus. The transaction flow in the HLF protocol is illustrated in Figure 4 [41,42,43,44].

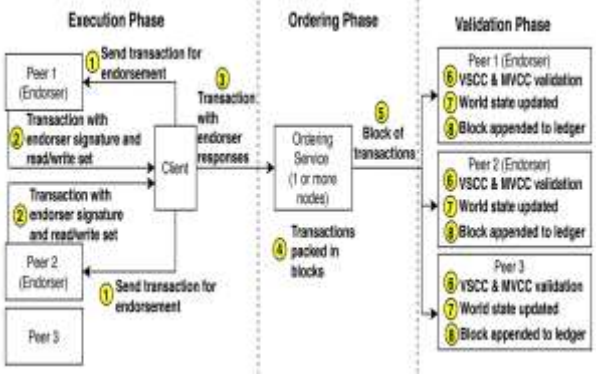

Figure 4. *Transaction flow in HLF protocol [41].*

Within the Hyperledger Fabric protocol, the creation of a new block prompts the need for its dissemination to other peers, which subsequently embark on the block's validation process. During this validation journey, peers initiate the verification by examining the ordering node's signature on the new block. This is followed by the block's deconstruction to unveil its embedded transactions. Moving forward, each transaction within the fresh block encounters two distinct validation phases: VSCC (Validation System Chaincode) validation and MVCC (Multi-Version Concurrency Control) validation. During the VSCC validation phase, peers undertake an assessment to ensure that the endorsements contained within the transaction align with the prescribed endorsement policy. Successful alignment results in verification success, thereby classifying the transaction as valid.

Conversely, misalignment designates the transaction as invalid. In the MVCC validation phase, peers delve into verifying whether the version of the key noted during the endorsement phase matches the version of the key stored within the current state database. A divergence in these versions signifies modification of a previous transaction, rendering it void. The data housed within the block is enveloped in a multi-layered structure. Accessing the data requiring verification necessitates multiple instances of deserialization of the block, a process characterised by substantial time consumption [39,43].

2.4 InterPlanetary File System (IPFS)

IPFS, denoting the InterPlanetary File System, signifies an intricate amalgamation of modular protocols poised to revolutionise extant conceptions of data organisation and transmission. Conceived with a confluence of content addressing and peer-to-peer networking principles, IPFS emblemizes a paradigmatic shift towards an unprecedented data regime. Within the open-source milieu, IPFS flourishes as a variegated tapestry of implementations, engendering a prolific ecosystem endowed with manifold possibilities. Paramount among its manifold applications is the pivotal function of effectuating decentralised data publication, thereby conferring agency over the dissemination of diverse data modalities such as files, directories, and comprehensive web entities, all within an inherently decentralised framework [45].

In its elemental configuration, IPFS assumes the character of a dynamic file system, underpinned by a meticulously architected distributed hash table (DHT) infrastructure. This construct, characterised by its capacity to facilitate seamless traversal and propagation of content-associated data units, demarcates IPFS from solutions confined by narrower storage methodologies or singularly purposed missions. Notably, Filecoin, intrinsically enmeshed within the IPFS fabric, harnesses its infrastructure for data archival and retrieval, culminating in a harmonious amalgamation that exudes the virtues of decentralised and highly efficient storage solutions. Subsequently, Hypercore, a prominent instantiation, emerges as a decentralised data-sharing paradigm, sustained by the very DHT substratum. Its vocation, however, veers towards fostering a milieu conducive to frictionless data interchange and dynamic collaborative endeavours. Swarm, an offspring of the Ethereum blockchain, ascends as a vanguard of decentralised purview. Orchestrating its ambitions through smart contracts and cryptographic artistry, it materialises as an impregnable repository of data integrity. It aspires to redress the exigencies of decentralised, immutable, and impermeable data custody, thus inaugurating an epoch of unwavering data stewardship[46].

In elucidating what IPFS does not signify, one is compelled to acknowledge its multi-dimensional essence. Resonating with the demeanour of a protocol, IPFS eschews the role of an autonomous storage proponent. Although symbiotic interludes transpire with storage providers, commonly referred to as "pinning services," IPFS maintains its quintessence as a symphonic architect rather than a custodian of data reservoirs. Similarly, in its interface with the cloud milieu, IPFS assumes the character of a gentle drizzle, complementing the overarching ambiance without masquerading as a preeminent cloud service provider [46,47].

2.5 Vernam Cipher

The Vernam Cipher, also known as the One-Time Pad (OTP), stands as one of the most intriguing and theoretically unbreakable encryption techniques. Its foundation lies in the concept of perfect secrecy, where an encrypted message provides no information about the original message, even to an adversary with unlimited computational power. This remarkable property stems from the fact that each character or bit in the plaintext is combined with a random character or bit from the key using the XOR operation. This results in an output that is seemingly random and offers no statistical patterns to exploit. One of the core challenges in utilising the OTP is the key management process. Each key used for encryption should be truly random and should be as long as the message itself, and produced for each encryption process uniquely. Key generation requires a trustworthy source of entropy, often derived from physical processes such as electronic

noise or radioactive decay. Additionally, securely distributing these lengthy keys to both the sender and receiver is paramount, as any compromise in the key exchange process could undermine the security of the entire system. The concept of the OTP has remains resilient even in the face of advancements in cryptography, including the advent of quantum computing. Unlike many other encryption methods that can potentially be broken by quantum computers due to their ability to efficiently factor large numbers, the OTP remains secure due to its unique properties and the fundamental principles on which it is built. To illustrate the OTP process, refer to Figure 5, which visually represents the steps involved in this encryption technique. This visualisation can help readers grasp the concept more easily and appreciate the elegance of the algorithm [48].

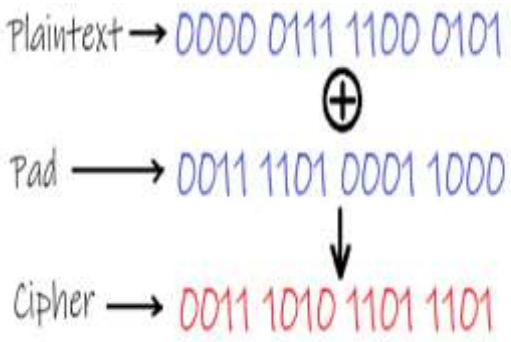

Figure 5. *Steps of One-Time-Pad symmetric encryption.*

2.6 OTA 1.0

The OTA 1.0 algorithm is a private blockchain system formulated for covert communication through steganography. It has been constructed from the ground up using Java and JavaScript programming languages. As a private blockchain, entry into the OTA 1.0 system mandates authorization. Initially, 50 OTA tokens are apportioned to approved node wallets. The fixed cost for each transaction within the system is 1 OTA token. This proposed algorithm comprises two main phases: first, the steganography process, followed by the transmission of stego-data using the private OTA-chain blockchain system [20].

2.6.1 OTA 1.0 Steganography Algorithm

In the proposed OTA-steganography algorithm, the chosen multimedia items serving as covers are securely stored on a dedicated server. The URLs associated with these multimedia elements are then logged and saved within the OTA-chain blocks. This strategy enables the detection and rectification of inadvertent alterations that might occur during the transmission of the cover multimedia through public channels. Unlike traditional steganography methods, the OTA-steganography algorithm abstains from concealing data within the cover multimedia image, rendering it impervious to steganalysis techniques. Thus, it stands apart from conventional approaches, boasting its own distinctive structure [20].

The process involves segmenting the plaintext data into varying numbers of bits, such as 2, 3, 4, and so forth, depending on the predetermined chunk size. Regardless of the chosen division, the algorithm undertakes systematic matches for bit patterns within the cover multimedia file to locate matching fragments of bits. Once a match is found, the algorithm records the starting bit position, or index, within the cover multimedia. Subsequent searches for remaining bit fragments continue from where the last successful search concluded, ensuring continuity [20].

If a search for a specific plaintext bit fragment traverses the entire cover multimedia without discovering the intended bit pattern, the search recommences from the file's inception, creating a cyclic process. As the algorithm successfully identifies all bit patterns from the plaintext data within the cover multimedia, the corresponding indices are compiled into an array known as the "address array." This array is further divided into kilobyte-sized segments, with each 1 kB of stego-data aligning with a single transaction within the OTA-chain. Figure 6 illustrates the architecture of the OTA-steganography algorithm [20].

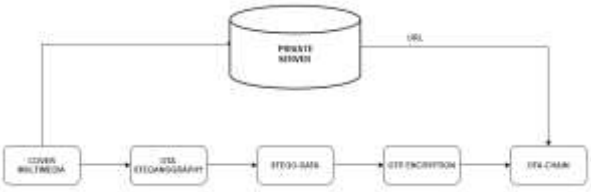

Figure 6. *The architecture of OTA steganography [20].*

During the processing of the cover multimedia by the OTA-steganography algorithm, indices corresponding to 2, 3, and 4 bit fragments of the plaintext data are retained for the sake of performance assessment. Opting for larger fragments leads to a reduction in the size of the address array, yet it entails increased search time during the creation of this array. The stego-data, which in this context refers to the address array, generated by the OTA-steganography algorithm, undergoes encryption utilising the One-Time-Pad (OTP) algorithm. Sharing the OTP key can be executed through any means, as the OTA-chain's private blockchain structure mitigates any potential risks stemming from unauthorised possession of the key by malicious entities via public channels.

Despite the algorithm's initial design for smaller message sizes, its cyclic nature enables the transformation of data larger than the cover multimedia file into an address array [20].
The proposed OTA-steganography algorithm achieves an extensive payload capacity, courtesy of its unique approach involving precise marking and indexing of a single cover multimedia [20].

2.6.2 OTA(1.0)-Chain Algorithm

Crafted with a specific focus on meeting steganographic demands, the OTA-chain algorithm has been purposefully developed. Within the OTA-chain network, nodes harbouring steganographic information can establish secure intercommunication. Notably, conventional platforms like Bitcoin, and Ethereum blockchain platforms have been deliberately eschewed. This strategic choice is predicated on the objective of maintaining streamlined system costs, a rationale expounded upon earlier. Given the OTA-chain system's reliance on OTA coins, the transmission of an OTA coin alongside stego-data to the recipient serves a dual purpose. This OTA coin within the recipient's wallet acts as both a reminder and a cautionary message for the user. Effectively, the mechanism of sending the coin operates akin to a ring, functioning as a notifier for the recipient and also preventing DDoS attacks due to transaction costs [20].
Of paramount significance, the OTA coin is disbursed to eligible nodes without any associated cost, thereby constraining the system expenses solely to the processing capability offered by the participating nodes' hardware. Pioneering the development of the OTA-chain algorithm from the ground up facilitated the early integration of numerous essential functionalities into the system. The block framework of the proposed system, meticulously tailored to meet steganographic requisites, encompasses key components such as the sender address, receiver address, timestamp, last hash, hash, nonce, difficulty, URL, and data [20].
The OTA-chain algorithm introduces a concept of a private blockchain system, wherein unauthorised entities lacking access permissions are precluded from scrutinising transactions. The stego-data, once transmitted, undergoes OTP algorithm encryption and is subsequently inscribed into the system's blocks. This measure ensures that the system's nodes, which hold access privileges, remain inaccessible to malevolent entities and impervious to potential manipulations or insider attacks. Nodes exclusively possess the capability to review transactions confined within the OTA-chain system.
The proposed algorithm employs the Proof-of-Work consensus mechanism. The system's constituent nodes also serve as miners, and those bestowed with block writing authority are rewarded with 50 OTA coins. Moreover, a minimum transaction cost of 1 OTA coin has been established for activities on the OTA-chain. Each transaction, spanning up to 1 kB in size, corresponds precisely to 1 OTA coin. The stego-data integrated into the OTA-chain consists of 1 kB Ciphered Secret Data (CSD) encrypted arrays produced during the OTA-steganography phase. This arrangement segments encrypted data into 1 kB blocks, with the transaction count aligning with the quantity of these confidential data blocks [20].
The OTA-chain algorithm embodies an on-chain blockchain system. Information pertaining to the system's data is logged within OTA-chain blocks. Unlike analogous endeavours, the system blocks refrain from concealing image matrices, which optimises both time and processing efficiency. Notably, the proposed system sidesteps the costs associated with pre-existing platforms featured in prior literature studies. Within the OTA-chain framework, secure sharing of the URL address of the desired cover multimedia for purchasers is achieved, alongside encrypted stego-data. A schematic depiction of the OTA-steganography and OTA-chain architecture inherent to the OTA algorithm is presented in Figure 7 [20].

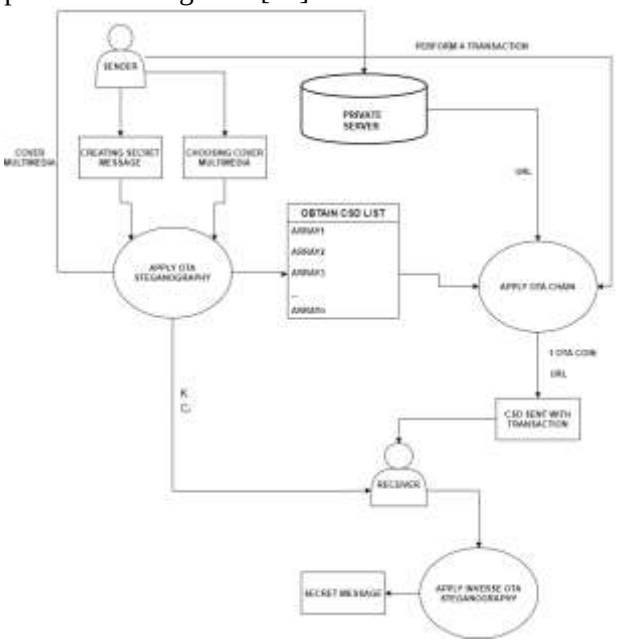

Figure 7. *Structure of OTA(1.0) algorithm [20].*

3. OTA 2.0

In the work, a new and improved system has been proposed with the aim of popularising and enhancing the applicability of the blockchain-steganography method recommended in OTA 1.0. In the proposed OTA 2.0 method, the Hyperledger Fabric protocol

has been used. Due to HLF being a permissioned platform, access permissions of users can be easily controlled. Furthermore, in OTA 2.0, access to the system can be achieved using Decentralised Identifiers (DID). The usage of TÜBİTAK BİLGEM's DID SDK (Indy) is envisaged in the proposed system. As HLF has a modular structure, it allows integration of various DID solutions. For the ease of use and widespread adoption of the proposed OTA 2.0, it is planned to be developed as a mobile application. Senders and recipients can transmit the desired types of files as steganographic cover-multimedia, embedding the secret message they want to convey in a way that does not cause any changes to the cover. The mobile application will be designed to have a simple and practical user interface. The OTA system will generate a DID for users registered in the system and associate it with their wallets. However, the verification and KYC processes of registered users have been kept out of scope in the study. Organisations wishing to implement the proposed method can make adjustments according to their needs and the scenarios they will use.

From a user perspective, using OTA 2.0 is quite simple. To send a secret message to the recipient's wallet address, they will select a file or take a photo from their phones and send it along with the message. There is no transaction cost associated with this process, and the recipient will receive an informational message (notification) indicating that they have received the information. The recipient must reach this message within 3 days; otherwise, access to the sent secret message will not be possible. This designated 3-day period can be changed up to 30 days. However, in the study, files are not planned to be pinned in IPFS, and as a result, files will be deleted from IPFS after a maximum of 30 days. Additionally, in steganographic processes, since the significance and validity of information are limited, it is crucial for the transmission of confidential data to be completed as quickly as possible in the process, leaving no meaningful trace behind. In addition to the deletion of non-pinned files in IPFS, due to the innovative key distribution method proposed in the study, the keypool creation seed used will be deleted from HLF after 3 days. As a result, accessing the key to the file encrypted with OTP will become impossible, rendering the received data unreadable by the recipient. Figure 8 illustrates the overall architecture of the proposed OTA 2.0 algorithm. Although OTA 2.0 is a permissioned system, and even though users granted access to the system are limited to sending data and reading incoming data only through mobile applications, the encrypted form of Secret Data using OTP is planned to be concealed through the OTA-steganography

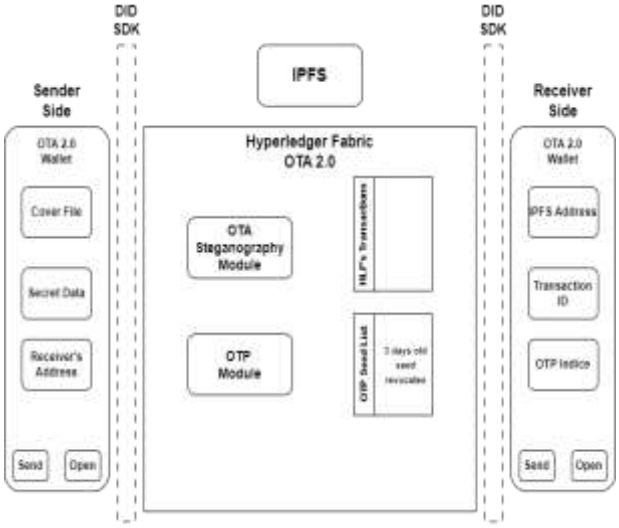

Figure 8. *Structure of OTA(2.0) algorithm.*

algorithm within HLF. This approach aims to prevent possible insider attacks by utilising the marked bit indices stored in HLF transactions. Furthermore, to counteract potential insider attacks, the cover-multimedia files stored in IPFS have been uploaded without pinning to ensure their deletion from IPFS after 30 days.

In the proposed OTA 2.0 study, an innovative key generation and distribution method for OTP has been suggested. The keypool is created on HLF using a randomly selected seed value. The chosen seed values are generated on an hourly basis, and the seed value generated for each hour is kept in the OTP Seed List. Seed values stored in the OTP seed list are removed from the list if they exceed 72 hours. To start from a randomly chosen point in the created keypool and cover the size of the data to be concealed, a key is selected, and the secret data is XORed. The index information of the selected key point is recorded for communication to the recipient. With this proposed method, the encryption process occurs within HLF's chaincode, and the key distribution process is carried out without sharing the key itself. If the receiver attempts an insider attack on the system, they cannot access the HLF transaction data, and since they cannot generate the keypool's seed value from the received key selection point index without the seed, they cannot use it to execute a successful attack. This lack of usability prevents any potential risks. Due to the deletion of the seed value after 72 hours, the key cannot be obtained, ensuring security against any type of attack that might be directed at the system. Figure 9 illustrates the encryption architecture of the OTP module, while Figure 10 shares the decryption architecture of the OTP module. The OTA-Steganography algorithm introduced in OTA 1.0 has been utilised in OTA 2.0 with slight differences.

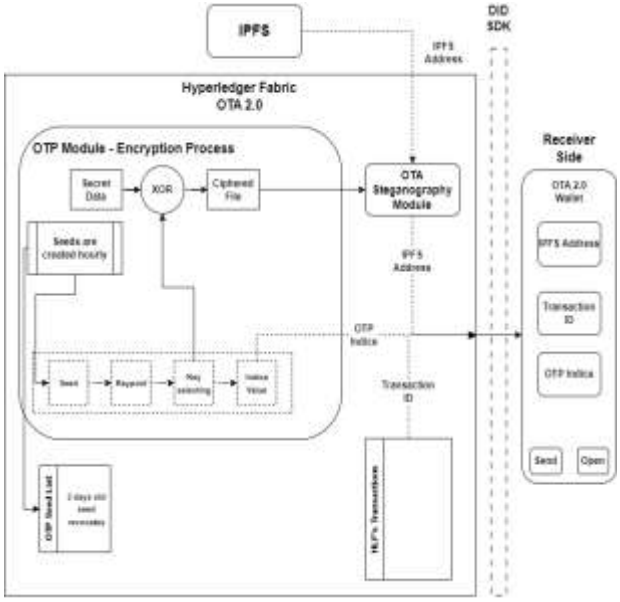

Figure 9. *Structure of encryption process.*

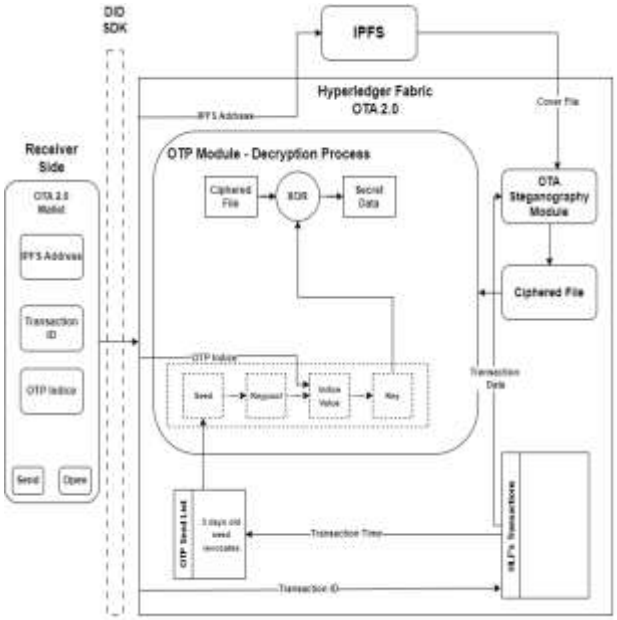

Figure 10. *Structure of decryption process.*

In the previous version, data embedding was performed with 4-bit, 6-bit, 8-bit, and 10-bit patterns. However, in OTA 2.0, it was decided to use only a 4-bit data embedding.

The calculation of the likelihood of not encountering a bit pattern of size n within cover multimedia of length m, where m is greater than n, is achieved through Markov chains. Specifics regarding bit patterns of varying lengths, cover multimedia length, and their associated probabilities are outlined in Table 1. As seen in the table, it is seen that the data embedding performed using 4-bit patterns yields quite successful results. The process of a blockchain-steganography operation in OTA 2.0 follows these steps:

Table 1. *The likelihood of discovering an n-bit pattern within an m-bit cover multimedia.*

	128 Byte	**256 Byte**	**512 Byte**	**1 kB**	**4 kB**
4-bit	~100%	~100%	~100%	~100%	~100%
6-bit	99.99%	~100%	~100%	~100%	~100%
8-bit	98.35%	99.98%	99.99%	~100%	~100%
10-bit	64.10%	85.45%	98.81%	99.91%	~100%

1. **User Registration in OTA 2.0:** After installing the OTA 2.0 mobile application, users complete their KYC processes and are provided with verifiable credentials for their wallets.
2. **Cover-Multimedia Selection:** Users can select files of various types. The chosen file is uploaded to IPFS through the mobile application, and the IPFS link is sent to OTA 2.0.
3. **Entering Secret Data:** The confidential data intended for transmission is input at this stage. While there is no specific limitation on the size of Secret Data, its size is expected to be relatively small due to the nature of steganographic processes.
4. **Entering Receiver Address:** The recipient's wallet information needs to be provided to the mobile application.
5. **Initiation of Sending Process:** Once cover-multimedia, secret data, and receiver address data are entered, the sender requests the transmission to the recipient through OTA 2.0 using APIs.
6. **Identity Verification:** Whenever OTA 2.0 interacts with users, it first verifies the verifiable credential (VC) of the requesting sender. This step may increase processing time but is crucial for security. The system ensures the validity of the user's access permission. Upon validation, the user's request is processed.
7. **IPFS Interaction:** The cover-multimedia IPFS link from the received transaction request is used to access the file. The cover-multimedia is sent to the OTA-Steganography module.
8. **KeyPool Creation:** A new random seed is generated every hour, and random numbers are generated and used as keys using these seed values. The seed value generated for each hour is written to the OTP Seed List. Seed values exceeding 72 hours are removed from this list.

9. **Encryption of Secret Data:** The secret data provided by the sender is XORed with a key selected from the keypool created using the Vernam Cipher. The size of the key matches the size of the secret data. A random point is selected from the keypool to read the key. The index of the selected point is recorded for the recipient, completing the encryption process.
10. **OTA-Steganography Process:** The cover-multimedia retrieved from IPFS and the encrypted secret data from the OTP module are concealed using 4-bit patterns. The indices of matching bits are recorded, and this information is written in the data block of the sent transaction. Only one transaction's data is allowed to be recorded in each block. The block creation time in HLF is set at 2 seconds, which can be adjusted if needed. The block size is set to 90 MB, which is sufficient for steganographic processes.
11. **Sending Notification to Receiver:** After completing its operation, the OTA-Steganography module triggers a transaction in HLF, creating a block. Subsequently, the OTP index value, transaction ID, and IPFS address are sent to the recipient, and a notification is sent to their mobile wallet.
12. **Receiver's Request for Accessing the Secret Data:** Upon receiving the notification, the recipient requests to access the received secret message. The recipient's VC is checked, as there is a possibility they could be added to the revocation list during the time that has passed. If the recipient has a valid VC, HLF processes the incoming request.
13. **Accessing Cover-Multimedia from IPFS:** Using the IPFS link in the recipient's digital wallet, the cover-multimedia is accessed and sent to the OTA-Steganography module.
14. **Utilising Transaction ID:** Using the Transaction ID provided by the recipient, information about the bit indices marked with 4-bit patterns is retrieved from the ledger. Additionally, the date and time information of the transaction indicated by the Transaction ID is used to check the OTP Seed List. If less than 72 hours have passed, the seed value is sent to the OTP decryption module.
15. **Locating the Ciphered File:** After providing the cover-multimedia and the indices marked with patterns to the OTA-Steganography module, the encrypted secret data file is obtained from the cover-multimedia using the bit indices. This ciphered file is then sent to the OTP module.
16. **Locating the Secret Data:** To unlock the ciphered file provided to the OTP module, the key needs to be re-generated. To achieve this, the keypool used at the time of file encryption is reconstructed using the seed value. The key is read from the keypool based on the index of the selected point, which is then used to perform an XOR operation and access the secret data. The retrieved Secret Data is then sent to the receiver.

Another advantage of implementing the OTA 2.0 algorithm within the Hyperledger Fabric protocol is the ease with which suspicious or unwanted users can be added to the revocation list. Furthermore, the MVCC mechanism inherent in the HLF protocol prevents DDoS attacks. The OTA 2.0 architecture is highly secure: All steganalysis methods are unable to detect blockchain steganography carried out through chaincodes. All types of files can be used as cover-multimedia, and data can be concealed without making any modifications to the files, without any issue of hiding capacity.

Neither Secret Data nor Cover-Multimedia are stored in HLF-ledger blocks. HLF-ledger blocks solely contain the indices of marked bits, which by themselves hold no meaningful information. After 72 hours (this duration can be extended or reduced), the transaction records registered in the system lose their utility. Files stored in IPFS, due to not being pinned, are deleted from the system within a maximum of 30 days, leaving behind no trace that can be detected.

Although the likelihood is extremely low, even if an attacker were to possess cover-multimedia, block data, and the OTA-Steganography algorithm simultaneously, they would be unable to acquire the same keypool without having the seed value (they lack direct access to the Seed list), and even if they had the seed value, they would not be able to obtain the same keypool without access to the same random number generator library used in the OTP module's chaincode, which is highly improbable. While this scenario is highly unlikely, user interactions with OTA 2.0 are restricted through mobile wallets, ensuring limited access to HLF block records. They cannot view other users' information beyond what is shown in their notifications. Moreover, all access to the system is managed through DID control, and user access is monitored.

The OTA 2.0 algorithm is designed within a permissioned architecture, which makes its distribution quality lower compared to a public blockchain project and somewhat centralised.

However, it provides a structure that perfectly addresses the needs of parties requiring blockchain steganography. The fact that HLF is an open-source platform and is regularly developed by an open-source community greatly facilitates the sustainability and improvement of the system. Additionally, HLF's modular structure, as demonstrated in the TÜBİTAK's DID SDK example, allows for the use of your own SDKs. In this context, for future cryptographic designs that may be required, they can be integrated into OTA 2.0 through HLF.

4. Discussions

The proposed OTA 2.0 Blockchain Steganography method aims to enhance the approach suggested in OTA 1.0. OTA 1.0 is significant for being the first method to propose steganography on a blockchain, thus contributing to the literature. OTA 1.0 consisted of two parts: OTA-Steganography and OTA-Chain. OTA-Chain was a newly developed private blockchain solution. In the OTA-Steganography phase, secret message data was matched to cover-multimedia data at the bit level using different bit patterns (4, 6, 8, 10), and the indices of the matching bits were stored in arrays that did not exceed 1 KB. These 1 KB arrays were sent to the recipient's wallet in OTA-Chain, with a fixed fee of 1 OTA-coin for the transaction. Upon registration, all users were provided with 50 OTA-coins, and the purpose of introducing a utilisation token was to prevent DDoS attacks. However, OTA 1.0 displayed weaknesses due to its lack of open-source nature, absence of support from an open-source committee, and therefore, its inability to create a usage example.

Additionally, OTA-Chain couldn't be developed further in terms of software after it was proposed, and monitoring and benchmarking tools couldn't be prepared. For all these reasons, the aim was to implement the blockchain steganography method from OTA 1.0 on a different platform and overcome the encountered issues. In this context, in this prepared study, the OTA-Steganography and OTA-Chain approach has been restructured using the Hyperledger Fabric protocol. Moreover, innovations such as the decentralised identifier extension and OTP key generation and distribution have been added to the system.

In OTA 2.0, OTA-Chain has been replaced with Hyperledger Fabric. In this context, the use of OTA-Coin has been discontinued, and a new model has been introduced that has no transaction fees and utilises the internal mechanism of HLF (MVCC) to guard against DDoS attacks. OTA-Steganography, on the other hand, is proposed as a chaincode (OTA-Steganography Module) within HLF, and simultaneously, marking using a 4-bit pattern is suggested. The selection of the 4-bit pattern, as seen in Table 1, has proven to be effective in achieving almost 100% probability of marking for nearly all file sizes.

All file types are compatible with the OTA-Steganography module. This is because all file types are read at the bit level, enabling blockchain steganography to be carried out by marking these bits. Additionally, the cover-multimedia chosen by the user comes from IPFS, and cover-multimedia files are not stored in HLF. This approach aims to enhance steganographic security and system scalability. Files stored in IPFS are not pinned, limiting the duration of cover-multimedia retention on IPFS to a maximum of 30 days. Given the importance of quickly transmitting data to the recipient in steganographic processes, long-term data storage is unnecessary. Therefore, in the process of creating the OTP keypool, which is another important development in the system, the seed values used are irreversibly deleted from the system after 72 hours, aligning with the spirit of steganography.

Similarly, the size of the hidden data sent to the recipient is generally very small, adhering to the essence of steganography. However, in the system, a significant improvement has been made by allocating a 90 MB block size for each transaction, enabling the transmission of larger hidden data sizes. The block creation time in HLF is set to 2 seconds, and the block size is set at 90 MB. As a result, the use of a 1 KB array is no longer necessary. Just like in OTA 1.0, OTA 2.0 ensures that no degradation occurs in the cover-multimedia. Subjecting the cover-multimedia stored in IPFS to steganalysis methods doesn't pose any security vulnerability and remains undetectable.

The OTP encryption algorithm, being a highly secure symmetric encryption method, has been utilized in OTA 2.0, just as it was in OTA 1.0. A different approach has been taken in generating the key that needs to be chosen for the size of the file to be encrypted. In the OTP module, a seed value is generated every hour to create a changing keypool. This keypool is accessible only at the chaincode level of HLF. The generated seed values are stored in the OTP-Seed List for 72 hours before being deleted. From these created keypools, a random starting point is selected, and key selection is performed for the size of the file. The secret data is encrypted using this key, and the index value of the key selection is recorded to be transmitted to the recipient. This proposed solution deviates from conventional key distribution methods, aiming to mitigate security vulnerabilities that might arise in traditional key distribution processes.

If the recipient wishes to access the data sent after receiving the notification within 3 days, they provide the OTP index, transaction ID, and IPFS address to OTA 2.0 to access the secret data. In this process, the seed value used at the time of the transaction is employed to recreate the keypool, and using the OTP index information, the key is obtained. By applying reverse OTA-Steganography, the ciphered document is obtained, decrypted using the key, and then conveyed to the user. Throughout this process, the user merely needs to possess a valid verifiable credential and make requests through OTA 2.0's APIs via their mobile wallet.

The Hyperledger Fabric protocol is not particularly efficient in terms of speed. The proposed DID integration and the necessity for DID verification in every transaction, along with the communication between the Mobile Wallet and OTA 2.0 and IPFS through APIs, will lead to lower TPS (transactions per second) rates in the system. However, OTA 2.0 does not require the high TPS typically needed in financial solutions. The fact that transaction processing times are not very short is not considered a significant issue. The system's performance can be monitored through benchmarking and monitoring tools. The proposed OTA 2.0 algorithm in this study possesses a significantly superior infrastructure and security features compared to its predecessor, OTA 1.0. The integration of the Mobile Wallet extension also paves the way for OTA 2.0 blockchain steganography to be easily accessible to end-users. The user base for the OTA 2.0 algorithm is highly specific and limited. Therefore, the realisation and maintenance of OTA 2.0 would require a considerable investment from an organisation. The OTA 2.0 algorithm, as suggested by the expert teams at TÜBİTAK BİLGEM UEKAE BZLAB, and professors from Istanbul Atlas University is being developed for testing purposes and in a secure environment as part of BZLAB's R&D activities. However, there are no plans to offer it as a final product to users. The implementation of the proposed OTA 2.0 algorithm in this study has not been fully completed. Therefore, tests and analyses, including system speed and cybersecurity analysis, are not currently available for sharing.

4. Conclusion

In essence, OTA 2.0 signifies a notable leap ahead of its precursor, tapping into the capabilities of the Hyperledger Fabric protocol. This evolution ushers in a spectrum of benefits, encompassing open-source availability, permissioned blockchain solutions, decentralization, and endorsement of self-sovereign identity. Furthermore, the algorithm's enhancements, including quicker block creation, expanded block size, and integration of a 4-bit marking pattern, amplify its effectiveness. Through the removal of transaction fees and the introduction of an inventive key-sharing methodology within its permissioned framework, OTA 2.0 adeptly thwarts conventional steganalysis techniques. This pioneering technology empowers the seamless and secure embedding of confidential messages across diverse multimedia formats.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare their acknowledgment to the TÜBİTAK-BİLGEM-UEKAE-Blockchain Technologies Department (BZLAB).
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] Takaoğlu, M., Özyavaş, A., Ajlouni, N. & Takaoğlu, F. (2023). Highly Secured Hybrid Image Steganography with an Improved Key Generation and Exchange for One-Time-Pad Encryption Method. *Afyon Kocatepe Üniversitesi Fen Ve Mühendislik Bilimleri Dergisi.* 23(1):101-114. DOI:10.35414/akufemubid.1128075

[2] Şahin, F., Çevik, T. & Takaoğlu, M. (2021). Review of the Literature on the Steganography Concept. *International Journal of Computer Applications.* 183(2):38-46. DOI:10.5120/ijca2021921298

[3] Takaoğlu, F. & Takaoğlu, M. (2020). Hiding Image and Text Data with DCT and DWT Techniques. *Journal of İstanbul Aydın University*. 12(3):189-200. DOI:10.17932/IAU.IAUD.2009.002/iaud_v12i3001

[4] Takaoğlu, F. & Takaoğlu, M. (2020). Today's Validity of Printer Steganography and Yellow Dot Analysis. *e-Journal of New Media / Yeni Medya Elektronik Dergi-eJNM.* 4(3):186-194. DOI:10.17932/IAU.EJNM.25480200.2020/ejnm_v4i3004

[5] Takaoğlu, M., Özer, Ç. & Parlak, E. (2019). Blockchain Technology and Possible Application Areas in Turkey. *International Journal of Eastern Anatolia Science Engineering and Design.* 1(2):260-295.

[6] Chaum, D. (1983). Blind signatures for untraceable payments. *Advances in Cryptology Proceedings of Crypto.* 82(3):199-203. DOI:10.1007/978-1-4757-0602-4_18

[7] Szabo, N. (2008). *Bit Gold*. http://unenumerated.blogspot.com/2005/12/bit-gold.html

[8] Fanning, S., Parker, S. & Contreras, H. S. (1999). *Nabster*. https://en.wikipedia.org/wiki/Napster_(streaming_service)

[9] Frankel, J. & Pepper , T. (2000). *Gnutella*. https://www.gnutellaforums.com/

[10] Cohen, B. (2001). *BitTorrent*. https://www.bittorrent.org/

[11] Back, A. (1997). *Hashcash*. http://www.hashcash.org/

[12] Dai, W. (1998). *Bmoney*. http://www.weidai.com/bmoney.txt

[13] Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf

[14] Buterin, V. (2014). *Ethereum*. https://ethereum.org/en/whitepaper/

[15] Yakovenko, A. (2018). *Solana: A new architecture for a high performance blockchain v0.8.13*. https://solana.com/solana-whitepaper.pdf

[16] Kwon, J. (2014). *Tendermint: Consensus without Mining.* https://tendermint.com/static/docs/tendermint.pdf

[17] Sekniqi, K., Laine, D., Buttolph, S. & Sirer, E. G. (2020). *Avalanche Platform*. https://assets.website-files.com/5d80307810123f5ffbb34d6e/6008d7bbf8b10d1eb01e7e16_Avalanche%20Platform%20Whitepaper.pdf

[18] Ching, A. & Shaikh, M. (2022). *The Aptos Blockchain: Safe, Scalable, and Upgradeable Web3 Infrastructure.* https://aptos.dev/assets/files/Aptos-Whitepaper-47099b4b907b432f81fc0effd34f3b6a.pdf

[19] Chen, J. & Micali, S. (2017). *Algorand Theoretical Paper*. https://algorandcom.cdn.prismic.io/algorandcom%2Fece77f38-75b3-44de-bc7f-805f0e53a8d9_theoretical.pdf

[20] Takaoğlu, M., Özyavaş, A., Ajlouni, N., Alshahrani, A. & Alkasasbeh, B. (2021). A Novel and Robust Hybrid Blockchain and Steganography Scheme. *Appl. Sci.* 11:10698. DOI:10.3390/app112210698

[21] Takaoğlu, M., Takaoğlu, F. & Dursun, T. (2023, July 20-21). *NBS: An NFT-Based Blockchain Steganography Method.* Conference: the 2nd International Conference on Computing, IoT, and Data Analytics (ICCIDA), La Mancha-Spain. https://iccida.net/

[22] Chaudhary, A., Sharma, A. & Gupta, N. (2023). Designing A Secured Framework for the Steganography Process Using Blockchain and Machine Learning Technology. *International Journal of Intelligent Systems and Applications in Engineering*, 11(2s):96–103.

[23] Torki, O., Ashouri-Talouki, M. & Mahdavi, M. (2023). Hierarchical Deterministic Wallets for Secure Steganography in Blockchain. *The ISC International Journal of Information Security.* 15(1):73-81. DOI: 10.22042/isecure.2022.319074.729

[24] Chaudhary, A., Sharma, A. & Gupta, N. (2023). A Novel Approach to Blockchain and Deep Learning in the field of Steganography. *International Journal of Intelligent Systems and Applications in Engineering.* 11(2s):104–115.

[25] Jahnavi, S., Pradeep, S., Navtej, P., Medini, H.S. & Mamisha. (2023). Blockchain Technology Based Image Steganography. *International Journal of Innovative Research in Technology*. 9(12):637-642.

[26] Sarkar, P.; Ghosal, S.K.; Sarkar, M. (2020). Stego-Chain: A Framework to Mine Encoded Stego-Block in a Decentralized Network. *J. King Saud Univ. Comput. Inf. Sci*. 2020, 16, 25–29.

[27] Mohsin, A.H.; Zaidan, A.A.; Zaidan, B.B.; Mohammed, K.I.; Albahri, O.S.; Albahri, A.S.; Alsalem, M.A. (2021). PSO–Blockchain-Based Image Steganography: Towards a New Method to Secure Updating and Sharing COVID-19 Data in Decentralised Hospitals Intelligence Architecture. *Multimed. Tools Appl.* 2021, 80, 14137–14161.

[28] Li, D., & Kar, P. (2022). B-Spot: Blockchain and Steganography based Robust and Secure Photo Transmission Mechanism. *Journal of Mobile Multimedia*. 18(06):1677–1708. DOI:10.13052/jmm1550-4646.18610

[29] Basuki, A.I.; Rosiyadi, D. (2019). *Joint Transaction-Image Steganography for High Capacity Covert Communication.* In Proceedings of the 2019 International Conference on Computer, Control, Informatics and its Applications (IC3INA), Tangerang, Indonesia, 23–24 October 2019; pp. 41–46.

[30] Kandasamy, L. & Ajay, A. (2023). *Implementation of Blockchain Technology for Secure Image Sharing Using Double Layer Steganography.* In: Hu, Z., Wang, Y., He, M. (eds) Advances in Intelligent Systems, Computer Science and Digital Economics IV. CSDEIS 2022. Lecture Notes on Data Engineering and Communications Technologies, vol 158. Springer, Cham. DOI:10.1007/978-3-031-24475-9_16

[31] Partala, J. (2018). Provably Secure Covert Communication on Blockchain. *Cryptography.* 2(3):18. DOI:10.3390/cryptography2030018

[32] Horng, J. H., Chang, C. C., Li, G. L., Lee,W. K. & Hwang, S.O. (2021). Blockchain-Based Reversible Data Hiding for Securing Medical Images. *J. Healthc. Eng.* DOI:10.1155/2021/9943402

[33] Xu, M., Wu, H., Geng, G., Zhang, X. & Ding, F. (2019). *Broadcasting steganography in the blockchain.* In International Workshop on Digital Watermarking; Springer: Berlin-Heidelberg, Germany, 2019; pp. 256–267.

[34] Matzutt, R., Hiller, J., Henze, M., Ziegeldorf, J. H., Müllmann, D., Hohlfeld, O. & Wehrle, K. (2018). *A*

Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin. In Financial Cryptography and Data Security; Meiklejohn, S., Sako, K., Eds.; Springer: Berlin-Heidelberg, Germany, 2018; pp. 420–438.

[35] Giron, A. A., Martina, J. E. & Custódio, R. (2021). Steganographic Analysis of Blockchains. *Sensors.* 21(12): 4078. DOI:10.3390/s21124078

[36] Hashim, M. M., Rahim, M. S. M., Johi, F. A., Taha, M. S. & Hamad, H. S. (2018). Performance evaluation measurement of image steganography techniques with analysis of LSB based on variation image formats. *International Journal of Engineering & Technology*. 7(4):3505-3514. DOI:10.14419/ijet.v7i4.17294

[37] Al-Refai, S. & Al-Jarrah, M. M. (2020). *Secure Data Hiding Technique Using Batch Video Steganography*. In Proceedings of the 2019 2nd International Conference on Information Hiding and Image Processing (IHIP 2019). Association for Computing Machinery, New York, NY, USA, 1–4. DOI:10.1145/3383913.3383914

[38] Pinchen Cui, P., Guin, U., Skjellum, A. & Umphress, D. (2019). Blockchain in IoT: Current Trends, Challenges, and Future Roadmap. *Journal of Hardware and Systems Security*. 3(4):338-364. DOI:10.1007/s41635-019-00079-5

[39] Yan, T., Chen, W., Zhao, P. & et al. (2021). Handling conditional queries and data storage on Hyperledger Fabric efficiently. *World Wide Web*. 24:441–461. DOI:10.1007/s11280-020-00844-5

[40] Takaoğlu, M., Dursun, T., Doğan, A., Er, H., Bozkurt Günay, B., Emeç, C., Kumru, A., Demir, S., Kurt Toplu, S. & Özcandan, N. (2023). *The Impact of Self-Sovereign Identities on CyberSecurity.* IST-186-RSM, Specialist Meeting, Blockchain Technology for Coalition Operations. https://bilgem.tubitak.gov.tr/uekae-yayinlar/

[41] Khan, D., Jung, L. T., Hashmani, M. A. & Cheong, M. K. (2022). Empirical Performance Analysis of Hyperledger LTS for Small and Medium Enterprises. *Sensors.* 22(3):915. DOI:10.3390/s22030915

[42] Chacko, J. A., Mayer, R. & Jacobsen, H. A. (2021). *Why Do My Blockchain Transactions Fail? A Study of Hyperledger Fabric.* In Proceedings of the 2021 International Conference on Management of Data (SIGMOD '21). Association for Computing Machinery, New York, NY, USA, 221–234. DOI:10.1145/3448016.3452823

[43] Zhou, E., Sun, H., Pi, B., Sun, j., Yamashita, K. & Nomura, Y. (2019). *Ledgerdata Refiner: A Powerful Ledger Data Query Platform for Hyperledger Fabric.* Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), Granada, Spain, 433-440. DOI: 10.1109/IOTSMS48152.2019.8939212

[44] Ke, Z. & Park, N. (2022). Performance modeling and analysis of Hyperledger Fabric. *Cluster Comput.* DOI:10.1007/s10586-022-03800-2

[45] Song, M., Han, J., Eom, H. & Son, Y. (2022). *IPFSz: An Efficient Data Compression Scheme in InterPlanetary File System.* in IEEE Access. 10:122601-122611. DOI:10.1109/ACCESS.2022.3223107

[46] Benet, J. (2014). I*PFS documentation*. https://docs.ipfs.tech/

[47] Muralidharan, S. & Ko, H. (2019). *An InterPlanetary File System (IPFS) based IoT framework.* 2019 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 2019, pp. 1-2. DOI:10.1109/ICCE.2019.8662002

[48] Bennett, C. H., Brassard, G. & Breidbart, S. (2014). Quantum Cryptography II: How to re-use a one-time pad safely even if P=NP. *Nat Comput.* 13(4):453-458. DOI:10.1007/s11047-014-9453-6