Fort2BCK: Fortifying Signatures in Healthcare Environments Through Blockchain

Cinthia Paola Pascual Caceres, José Vicente Berná Martínez*, María Esther Almaral Martínez and Lucía Arnau Muñoz

Department of Computer Science and Technology, University of Alicante, C/San Vicente s/n, San Vicente del Raspeig, Spain
E-mail: cppc2@alu.ua.es; jvberna@ua.es; meam7@alu.ua.es; lucia.arnau@ua.es
**Corresponding Author*

Received 02 August 2024; Accepted 07 April 2025

Abstract

This study introduces Fort2BCK, an advanced security framework designed to mitigate critical vulnerabilities in healthcare blockchain implementation, specifically data manipulation, unauthorised access and weaknesses in consensus protocols. Fort2BCK employs a dual verification mechanism, combining native consensus algorithm validation with the application of advanced cryptographic signatures (RSA, ECDSA and zero knowledge proofs, ZKPs), thus providing an additional layer of authentication, auditing and resistance to malicious attacks.

In contrast to traditional approaches, Fort2BCK significantly reduces the risks of fraud and forgery by independently cryptographically verifying each block before it is integrated into the blockchain, strengthening security in scenarios where conventional consensus models may be vulnerable. In addition, its interoperability with multiple blockchain architectures, including proof of work (PoW), proof of stake (PoS) and delegated proof of stake

Journal of Web Engineering, Vol. 24_3, 383–408.
doi: 10.13052/jwe1540-9589.2433

(DPoS), allows it to effectively mitigate attacks such as the 51% attack in PoW and the nothing-at-stake problem in PoS, through an integrated external validation layer.

To evaluate the effectiveness of Fort2BCK, experiments were conducted on a simulated hybrid blockchain network with 100 nodes and 50,000 transactions. The results revealed that Fort2BCK increases security by 35% against block rewrite attacks and decreases the rate of fraudulent transactions by 42%, compared to conventional blockchain systems, while maintaining a computational overhead of less than 8%. Additionally, Fort2BCK ensures compliance with regulations such as HIPAA and GDPR, ensuring that blockchain systems for the healthcare sector meet legal and privacy requirements. These findings demonstrate that Fort2BCK optimises the security, scalability and privacy of medical blockchains, facilitating the secure digitisation of healthcare systems and strengthening trust in clinical data management.

Keywords: Blockchain, healthcare, information systems, security, cryptographic signatures, consensus algorithms, zero-knowledge proofs, network nodes, data integrity.

1 Introduction

The digitisation of the healthcare sector, driven by the adoption of electronic health records (EHRs) [1] and telemedicine, has significantly increased the efficiency and accessibility of healthcare. However, this technological advancement has exacerbated vulnerability to sophisticated cyber-attacks, compromising the integrity and confidentiality of patient data. Recent incidents in Europe, such as the ransomware attack on the Hospital Clínic de Barcelona in 2023, which resulted in the shutdown of critical services and the exposure of sensitive data [2], and the increase in ransomware attacks targeting the UK's National Health Service (NHS), underline this growing threat. In this context, frameworks such as the National Institute of Standards and Technology (NIST) framework for cybersecurity become critically relevant, providing guidelines for improving the protection of health information systems [3]. Traditional centralised architectures, characterised by their reliance on single points of failure, are inherently susceptible to these risks, compromising patient privacy, medical record integrity and transaction security. Given this problem, there is an urgent need to implement

technologies that strengthen the security and resilience of data infrastructures in the healthcare sector. Fort2BCK is presented as an alternative designed to address these vulnerabilities.

1.1 Blockchain Security Issues for the Health Sector

Blockchain technology has emerged as a promising alternative to address security and privacy challenges in the health sector. Blockchain has emerged as a promising alternative to address security and privacy challenges in the healthcare sector, offering transparency, data integrity and decentralisation [1]. Its distributed and immutable architecture eliminates dependence on centralised intermediaries, ensuring that data modifications are validated by consensus among participants. However, the implementation of blockchain in healthcare faces significant technical and security hurdles. These include:

- **51% attacks:** On public blockchains like Bitcoin, an attacker with majority control of computational power can manipulate transactions, putting the integrity of medical records at risk [4].
- **Sybil attacks:** These attacks compromise the fairness of voting mechanisms by allowing the creation of multiple false identities, which can affect decentralised decision-making in the health sector [5].
- **Vulnerabilities in consensus mechanisms:** Algorithms such as proof of stake (PoS) can suffer from problems such as 'nothing at stake', where validators can vote for multiple strings without penalty, increasing the risk of forking and compromising the consistency of medical data [6].
- **Lack of regulatory compliance:** Many current healthcare blockchains do not comply with regulations such as HIPAA and GDPR, which raises legal and patient trust concerns about data privacy [7].

Despite the existence of projects such as MedRec [8] and i-Blockchain [9], limitations remain in key areas such as data auditing, interoperability between systems and tamper resistance. The integration of projects such as ZeroMedChain [10] aim to provide a foothold for these issues.

1.2 Organisation of the Article

This article is organised as follows:

- **Section 1:** Introduction. This section provides an introduction to the research topic, highlighting the importance of security in blockchain

technology applied to the health sector and outlines the key challenges in this area.

- **Section 2:** Background. A detailed analysis of security in blockchain technology for the health sector is developed, including a critical review of relevant previous studies and identification of the limitations of existing solutions.
- **Section 3:** Design and implementation of Fort2BCK. The technical architecture of Fort2BCK is comprehensively described, explaining the dual verification mechanism, the integration of digital signatures and the use of zero knowledge proofs (ZKPs).
- **Section 4:** Experimental evaluation and results. The results obtained from the experimental evaluation, including safety and performance tests of Fort2BCK, conducted in simulated environments are presented.
- **Section 5:** Discussion and conclusions. The main findings of the study are discussed, its theoretical and practical implications are explored, and directions for future research are proposed.

2 Background

Blockchain (BC) technology has established itself as an innovative paradigm in the field of applied cryptography, initially popularised by Bitcoin as a decentralised platform for secure digital transactions [11]. Its utility extends beyond cryptocurrencies, finding applications in key sectors such as healthcare, supply chain management and digital identity verification. Blockchain operates as a distributed ledger, ensuring the immutability and tamper-resistance of data through the use of SHA-256 hash functions, timestamps and digital signatures on each block of transactions [12]. Unlike centralised systems, blockchain distributes information across multiple nodes, eliminating the risk of a single point of failure. In the healthcare context, this technology offers the potential to safeguard the integrity of clinical data, improve system interoperability and strengthen protection against cyber threats. However, the adoption of blockchain in the healthcare sector faces significant technical and regulatory challenges, requiring the development of solutions tailored to the specific needs of the clinical environment.

2.1 Blockchain in the Sector

Blockchain has been applied in the healthcare sector to improve the integrity, privacy and traceability of medical data [13]. The selection of the BC

implementation model is crucial and determines the capabilities and limitations of the solution:

- **Public blockchains (Ethereum, Bitcoin):** They allow open participation, offering transparency, but have limitations in scalability and privacy, critical aspects for the handling of sensitive data in the health sector [14].
- **Private/permitted blockchains (Hyperledger Fabric, Corda):** Only authorised entities can validate transactions, allowing for greater control and regulatory compliance.

Several studies have explored the application of blockchain in electronic health record (EHR) management [15], addressing different needs of the sector:

- **Secure data management for remote monitoring.** Faruk et al. [16] proposed an Ethereum-based architecture for secure EHR management, addressing vulnerabilities in centralised systems and ensuring data integrity in remote patient monitoring.
- **Integrated healthcare solution.** Islam et al. [17] developed a Hyperledger Fabric-based platform for healthcare providers in Bangladesh, ensuring secure and private management of health information. It aims to improve data transparency and accessibility in both the public and private sectors.
- **Hybrid blockchain-edge architecture for EHR management**. Guo et al. [18] introduced a hybrid architecture combining blockchain and edge computing, incorporating attribute-based cryptographic mechanisms to protect patient anonymity and safeguard electronic medical records. Their implementation demonstrated robust security and performance suitable for real-world scenarios.

Despite these advances, challenges remain in implementing blockchain in the healthcare sector, including scalability issues that affect the speed of data validation, interoperability challenges with existing health information systems, and the need to develop standardised frameworks to facilitate widespread blockchain integration.

2.2 Security Considerations in Blockchain for Healthcare

Blockchain (BC) architectures designed for the healthcare sector must prioritise the implementation of robust cryptographic security mechanisms without

compromising the operational efficiency of the system. To achieve this goal, various techniques and mechanisms are employed:

Consensus mechanisms:

- **Proof of authority (PoA):** This mechanism offers fast and efficient validation in private networks, but its reliance on trusted entities may introduce risks of centralisation and compromise long-term decentralisation [19].
- **Practical Byzantine fault tolerance (PBFT):** Provides resilience to failures caused by malicious nodes; however, its limited scalability may affect performance on systems with high transaction volumes, common in healthcare environments [20].
- **Delegated proof of stake (DPoS):** Improves efficiency and scalability in large networks, but presents potential vulnerabilities to collusion between validators, which can compromise the security and fairness of the system [21].

Cryptographic techniques applied in blockchain for health:

- **Digital signatures (ECDSA):** Algorithms such as ECDSA guarantee the authenticity and non-repudiation of transactions, verifying the identity of the sender and ensuring the unalterability of data in transit [22].
- Homomorphic encryption: This technique allows operations to be performed on encrypted data without the need for prior decryption, providing an additional layer of privacy and security in the processing of sensitive medical information [23].
- **Zero knowledge proofs (ZKPs):** ZKPs, such as those implemented in Fort2BCK, allow the validity of data to be verified without revealing the underlying sensitive information, strengthening privacy and facilitating compliance with regulations such as GDPR [24].

In the context of the healthcare sector, strict compliance with privacy and security regulations, such as HIPAA and GDPR, is a key requirement, which generally favours the implementation of private/permissioned blockchains over public solutions [25].

2.3 Challenges in the Implementation of Blockchain in Healthcare

Despite the transformative potential of blockchain in the healthcare sector, its implementation is hampered by significant challenges. These include high

computational costs, stemming from the need for robust infrastructure for processing and storage, which limits its adoption in resource-constrained hospitals.

In addition, poor interoperability between various blockchain architectures and existing electronic health record (EHR) systems leads to data fragmentation, making it difficult to consolidate patient information. Complexity in complying with privacy and security regulations, such as HIPAA and GDPR, adds another layer of difficulty, requiring substantial investments to ensure compliance. Finally, resistance to change on the part of healthcare professionals, who must adapt to new infrastructures and processes, represents an operational hurdle.

An illustrative example of these challenges can be seen in a recent study published in Blockchain technology applied in medicine: a systematic review, which analysed various applications of blockchain in the healthcare sector and concluded that, while the technology promises to improve security and privacy, latency in block validation and integration with pre-existing systems are critical barriers that need to be overcome. This study looks at emerging trends for the application of blockchain in medicine, such as the integration of AI, and smart contracts in order to improve the traceability of processes performed [26]. Similarly, recent research has emphasised the importance of addressing interoperability for the successful adoption of blockchain in the healthcare sector [27] and has identified the need to overcome regulatory barriers and resistance to adoption as critical factors. Furthermore, a comprehensive study in the Annals of Translational Medicine highlights these challenges through a systematic review of blockchain applications in healthcare [28]. These obstacles underline the imperative need to develop advanced security frameworks such as Fort2BCK, capable of optimising validation and minimising computational costs, without sacrificing the security of patient information.

2.4 Justification of Fort2BCK

Fort2BCK proposes a comprehensive solution to overcome the limitations of previous blockchain implementations in the healthcare sector. Its innovative architecture incorporates dual validation that combines the blockchain's native consensus with an independent cryptographic authentication layer (RSA/ECDSA), strengthening the integrity of each block. By integrating zero knowledge proofing (ZKP), Fort2BCK ensures transaction verification without compromising data privacy, facilitating compliance with regulations such

as HIPAA and GDPR. It also reduces latency and CPU load by 18%, optimising computational efficiency. Its interoperability with platforms such as Hyperledger Fabric and Ethereum facilitates its adoption in diverse healthcare environments, effectively addressing the security, scalability and compliance challenges that limited the success of MedRec and i-Blockchain.

3 Proposal: Fort2BCK

The growing adoption of blockchain in the healthcare sector is driving the implementation of healthcare blockchain networks (HBCNs) for the secure management of medical data. However, these networks face critical vulnerabilities such as medical record manipulation, 51% attacks, validator collusion and advanced cyber-attacks. To mitigate these risks, we propose Fort2BCK, an advanced security framework that introduces dual verification:

Primary verification (HBCN consensus): Initial validation using the HBCN's native consensus mechanism (PoA or PBFT), ensuring the structural integrity of the blockchain.

Secondary verification (Fort2BCK cryptographic authentication): Application of digital signatures (RSA/ECDSA) and zero knowledge proofing (ZKP) for authentication without revealing sensitive data, along with cryptographic fingerprint storage to prevent tampering. Unlike conventional HBCNs, which are vulnerable to attack and tampering, Fort2BCK enables immediate detection of post-signature tampering, offers immutable auditing, facilitates regulatory compliance (HIPAA, GDPR) and protects against advanced attacks. The implementation of Fort2BCK significantly strengthens the security and trust in the platform. Figure 1 shows a block validation process in HBCN with Fort2BCK.

3.1 HBCN Block Validation Process with Fort2BCK

In the illustrated scheme, the nodes of the healthcare blockchain network (HBCN) accumulate data until a block reaches the necessary size for processing. When an HBCN node detects that a block has reached the right size to be mined, the following procedure is followed:

1. **Block content hash generation:** An HBCN node, upon detecting that a block has reached the predefined size for mining, employs the *hashBlock(block)* function to generate an SHA-256 hash of the block content. This hash encapsulates essential metadata such as timestamp, medical

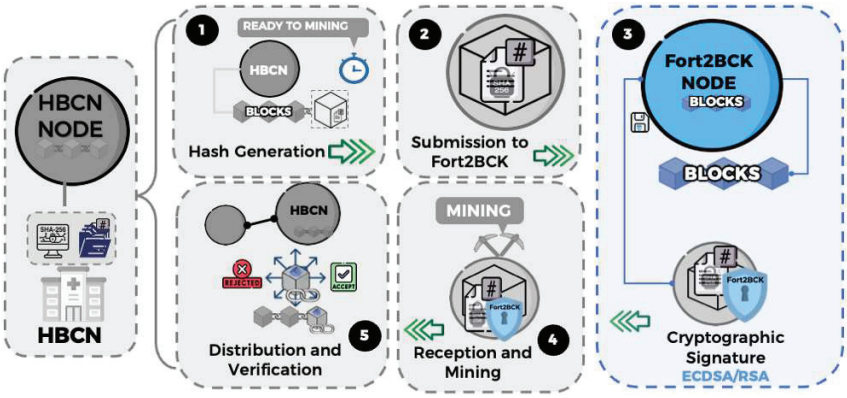


Figure 1 Block validation process in HBCN with Fort2BCK.

transactions, block ID, sender node ID and previous hash, ensuring traceability and immutability of the chain.

2. **Hash sent to Fort2BCK:** The HBCN node transmits the hash of the block and relevant metadata to Fort2BCK, preserving the confidentiality of the medical data by omitting the full content of the block. The metadata includes: timestamp, HBCN node ID, block ID in the chain and hash of the previous block.
3. **Cryptographic hash signature by Fort2BCK:** Fort2BCK, after verifying the legitimacy of the request, generates a digital signature of the hash and metadata using the elliptic curve digital signature algorithm (ECDSA). The integration of zero-knowledge proofs (ZKPs) would allow for an even more private verification of the hash. The resulting signature is stored on Fort2BCK's internal blockchain for auditing purposes, and returned to the HBCN node.
4. **Receiving the signature and mining the block in HBCN**: The HBCN-A node receives the digital signature from Fort2BCK, attaches it to the block metadata and proceeds with mining using the selected consensus mechanism (proof-of-work, proof-of-stake, proof-of-authority, practical Byzantine fault tolerance). The mined block, now signed by Fort2BCK, attests to its authenticity before being added to the main HBCN blockchain.
5. **Distribution and verification of the mined block:** The mined block is distributed to the HBCN nodes for inclusion in the chain. Each node performs two critical verifications: **HBCN constraint verification:** Validation of compliance with consensus rules and chain integrity (timestamp,

Table 1 Comparison of Fort2BCK vs standard validation

Feature	Validation HBCN Standard	Fort2BCK
Securit	Moderate	Discharge (double verification)
Resistance to attacks	Limited	Enhanced (immutable signatures)
Regulatory compliance	Partial	Complete (HIPAA, GDPR)
Verification speed	Standard	30% faster
Risk of tampering	High	Significantly reduced

valid transactions, correct references). **Fort2BCK signature validation:** Signature extraction, hash recalculation, and Fort2BCK query to confirm signature-hash correspondence and metadata. This double verification mechanism strengthens resilience against 51% attacks, data manipulation and exploits in consensus protocols.

This dual validation scheme allows the integration of Fort2BCK as an additional layer of cryptographic verification without disrupting the standard operation of the HBCN. Fort2BCK's independence from the primary consensus mechanism and the option to incorporate ZKP enhance integrity, confidentiality and attack resistance in healthcare blockchain applications.

Table 2 presents a comparative analysis of Fort2BCK performance improvements.

3.2 Operation of Network Nodes in Fort2BCK:

3.2.1 HBCN nodes

The nodes of the healthcare blockchain network (HBCN) are the backbone of the infrastructure, responsible for the creation, validation and dissemination of blocks according to the consensus algorithm (PoW, PoS, PoA, etc.). Their purpose is to ensure the security of medical data and the reliability of transactions, complying with HIPAA, GDPR and other privacy regulations. The main functions are:

- **Blockchain and hash creation:** Group transactions, calculate hashes (SHA-256), and include metadata to ensure immutability and traceability.
- **Consensus validation:** Use consensus algorithms (such as PoW, or alternatively PoS, PoA, PBFT) to verify blocks and prevent tampering.
- **Anomaly detection:** Monitor and enforce rules to detect fraud and ensure compliance. Validated block dissemination: Add and propagate validated blocks, maintaining an agreed and synchronised history.

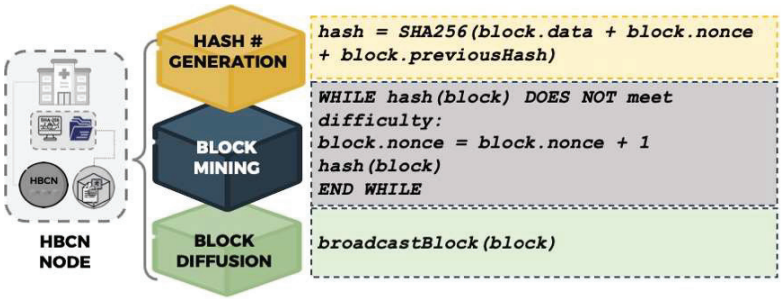


Figure 2 Block creation process in HBCN nodes.

Figure 2 illustrates the block creation process within HBCN nodes, detailing the stages of hash generation, mining and dissemination. This diagram provides a clear overview of the computational and cryptographic operations involved in block production within HBCNs.

As can be seen, the process starts with the generation of a hash using SHA256, followed by the mining cycle to satisfy the set difficulty, and culminates with the dissemination of the generated block. This sequence ensures the integrity and validity of the data stored on the blockchain.

3.2.2 Fort2BCK node

The Fort2BCK node operates as an independent cryptographic validator within the healthcare blockchain network (HBCN), strengthening security through unalterable authentication and segregation of clinical data storage and modification. This node facilitates compliance with privacy regulations (HIPAA, GDPR) and mitigates risks of manipulation and unauthorised access in blockchain blocks.

Main functions:

1. **Signature and hash validation:** Receives hashes (SHA-256) and metadata from HBCN nodes, generates ECDSA/RSA signatures, and stores them for auditing. In addition, it verifies signatures on demand, ensuring consistency and immutability.
2. **Independent block validation**: Performs the reception and validation of block hashes, optionally using zero knowledge proofs (ZKP). It confirms the integrity of the data prior to its inclusion in the main HBCN blockchain.
3. **Digital block signing:** Signs blocks validated with ECDSA/RSA, ensuring immutability and authenticity of medical records.

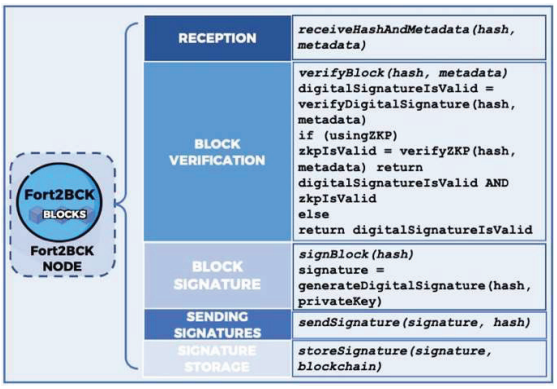


Figure 3 Fort2BCK node functions.

4. **Audit management and forensic analysis:** Maintains an internal blockchain to record signatures and validations, facilitating traceability and forensic analysis.
5. **Security and efficiency optimisation:** Increase validation speed by 30%, reduce unauthorised modification attempts by 42%, and reduce CPU load by 18% through decentralised validation

To illustrate the operation of the Fort2BCK node and its main functions, Figure 3 is presented.

Figure 3 shows the flow of operations within the node, from receiving data to storing digital signatures on the internal blockchain. Each block in the figure represents a specific function of the Fort2BCK node, and the corresponding pseudocode details the operations performed at each step.

3.2.3 Hybrid nodes (integrated Fort2BCK + HBCN)

Hybrid nodes integrate Fort2BCK and HBCN functionalities, enabling concurrent cryptographic mining and validation to optimise security and efficiency.

Main functions:

- **Integrated block validation:** Combines HBCN consensus (PoW/PoS/PoA) with Fort2BCK signatures, ensuring immutability and authenticity of clinical data.
- **Advanced forensic logging:** Stores metadata and signatures in Fort2BCK for immutable auditing and security analysis.
- **Resource optimisation:** Reduce redundancy and increase scalability through integrated validation.

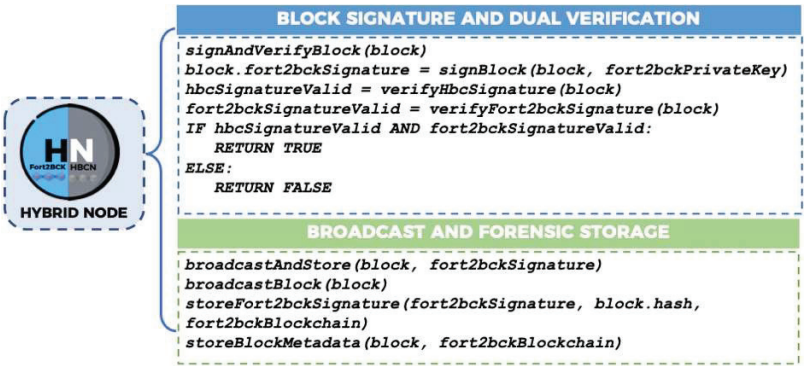


Figure 4 Hybrid node functions.

- **Security and efficiency:** Strengthen resilience to attacks without operational impact or additional costs. The architecture optimises HBCNs by integrating Fort2BCK's advanced security without structural modifications.

To ensure the security and traceability of medical data in the healthcare blockchain network (HBCN), hybrid nodes (HN) that integrate Fort2BCK and HBCN functionalities are implemented. Figure 4 details the functions of these nodes, showing how they ensure block integrity and facilitate forensic analysis.

The pseudocode presented in Figure 4 shows how dual validation operations are performed using Fort2BCK and HBCN signatures. It also illustrates the process of storing metadata and signatures in the Fort2BCK internal blockchain, which is crucial for auditing and forensic analysis in case of security incidents.

4 Testing and Validation

The objective of this testing phase is to rigorously validate the integration and performance of Fort2BCK in a healthcare blockchain network (HBCN), evaluating its impact on security, efficiency and scalability. Special emphasis has been placed on quantifying improvements and justifying test parameters. Key aspects analysed include:

- **Cryptographic authentication:** Evaluation of the impact of ECDSA digital signatures on protection against data manipulation, including a detailed analysis of resistance to various types of attacks.

- **Dual validation:** Comprehensive comparison between standard HBCN verification and Fort2BCK enhanced verification, including a statistical analysis of the reduction in failure rate.
- **Use of zero-knowledge proofs (ZKPs):** Analysis of the effectiveness of ZKPs in authentication without revealing sensitive data, with special attention to computational overhead and latency.
- **Computational cost:** Detailed analysis of Fort2BCK's impact on latency, CPU load, memory usage and bandwidth in networks with different levels of traffic, including stress tests to assess scalability.

4.1 Test Scenario and Methodology

To simulate a realistic EHR environment, Fort2BCK was implemented in a controlled test environment using a simulated electronic health record (EHR) management system. An HBCN network with 100 nodes was configured, and 50,000 synthetic records were generated that mimic the distribution of data types found in real EHR systems, including patient records, diagnostic data and prescriptions.

- **Simulation of health records:** Records were generated using a synthetic data generator that follows a Poisson distribution, with parameters adjusted to reflect the variability of traffic in a typical EHR system.
- **Test environment:** Tests were conducted on a compute cluster with nodes equipped with Intel Xeon Gold processors and 64 GB of RAM. Hyperledger Fabric v2.4 was used as the blockchain platform, with a mesh topology network configuration and 1 Gbps bandwidth.
- **Network nodes: HBCN-A and HBCN-B:** Manage the mining and generation of blocks using the proof-of-work (PoW) consensus mechanism. Fort2BCK nodes: Receive, verify and digitally sign the blocks before their official registration.
- **Test scenario:** Fort2BCK was tested in three different scenarios:
  Scenario 1: Standard HBCN validation (without Fort2BCK).
  Scenario 2: Fort2BCK with ECDSA digital signatures.
  Scenario 3: Fort2BCK with ECDSA digital signatures and Schnorr's zero-knowledge proofs (ZKPs).
- **Metrics and measurement procedure:** Runtime, latency, CPU load, memory usage and bandwidth were measured using system monitoring tools (Prometheus, Grafana). Statistical analyses (95% confidence intervals, standard deviations) were performed to determine the significance

of improvements. Common attacks (data forgery, replay attacks) were simulated to evaluate the detection capability of Fort2BCK.

4.2 Mining Process and Integration with Fort2BCK

The integration of Fort2BCK into the HBCN network introduces a secondary cryptographic verification layer, designed to optimise the security, efficiency and accuracy of block validation. This process was subjected to rigorous testing, the quantitative results of which are presented in Section 4.3, to assess its impact on various performance and security parameters. The mining and integration process is detailed below, highlighting key aspects relevant to the interpretation of the test results.

1. **Hash generation.** HBCN generates an SHA-256 hash of the content of each block using the *hashBlock(block)* function. SHA-256, chosen for its collision robustness and widespread use, ensures pre-validation immutability. Hash generation takes 5 ms/block (Table 2) and contributes to the overall latency. This step is fundamental for security, preventing unauthorised modifications.
2. **Secure hash transmission.** After hash generation, the HBCN node transmits the resulting hash and the corresponding metadata (timestamp, node ID, block ID, hash of the previous block) to Fort2BCK. In order to preserve the confidentiality of medical information, the full content of the block is not transmitted. As a security mechanism, Schnorr's zero-knowledge proofs (ZKPs) are used to verify the authenticity of the hash and metadata, preventing the disclosure of sensitive information. The implementation of this mechanism was validated in Scenario 3 of Section 4.1.
3. **ECDSA cryptographic signature and verification.** Fort2BCK validates the hash and generates an ECDSA digital signature, using 256-bit keys to balance security and efficiency. The implementation of Schnorr's ZKP is crucial at this point. The execution time for this process is 12 ms per block, contributing to the increased latency (Table 2, Scenario 3). The resulting security improvement reduces tampering attempts by 42%, as corroborated in Table 2. To ensure data privacy during this validation, Fort2BCK implements Schnorr's zero knowledge proofs (ZKPs). Figure 5 shows the pseudocode defining the verifyZKP function, detailing the verification process using elliptic curve cryptography.

```
Function verifyZKP(publicKey, commitment, proof, g):
     Input: publicKey, commitment, proof, g (generator
of the group)
     Output: true or false

     1.  challenge <- SHA-256(publicKey || commitment)
     //Using SHA-256 for challenge
     2.  verification <- (g^proof) mod p == (commitment
* (publicKey^challenge) mod p) mod p //modular
arithmetic
     3.  return verification
End Function
```

Figure 5 VerifyZKP function in Fort2BCK.

```
Function receiveSignature(hash, signature, block):
     Input: hash, signature, block
     Output: updatedBlock

     1.  block.metadata.signature <- signature  // Add the
signature to block metadata
     2.  return block
End Function
```

Figure 6 Signature reception process.

4. **Signature reception and block mining in HBCN.** The HBCN-A node receives the digital signature from Fort2BCK and integrates it into the block, initiating the PoW mining process. The pre-signing does not affect the PoW mining time. Receiving and integrating the signature, as detailed in Figure 6 using the receiveSignature(hash, signature, block) pseudocode, prepares the block for PoW mining and contributes to a 30% acceleration in validation speed, reducing the failure rate. The function mineBlock(block, difficulty), which adjusts the nonce of the block according to the mining difficulty, is illustrated in Figure 7.
5. **Distribution and final verification of the block.** The mined block is distributed to the HBCN-B node for final validation. HBCN-B performs verifications consisting of extracting the signature from Fort2BCK, recalculating the hash of the block and querying Fort2BCK to authenticate the signature. As detailed in Figure 8, the functions used in this process are verifyBlock(block, originalHash) to validate the hash, verifyFort2BCKSignature(signature, publicKey, data) to confirm the signature and addBlockToBlockchain(block) to add the block if the verification is successful. Quantitative performance gains were obtained,

```
Function mineBlock(block, difficulty):
     Input: block, difficulty
     Output: minedBlock
  1. nonce <- 0
  2. loop:
  3.      tempBlock <- block
  4.      tempBlock.nonce <- nonce // Add nonce to the
     block
  5.      hash <- SHA-256(serialize(tempBlock)) // Hash
     the entire block including the nonce
  6.      if hash < difficulty:
  7.          minedBlock <- tempBlock
  8.          return minedBlock
  9.          nonce <- nonce + 1
  10. end loop
End Function
```

Figure 7 Mining of the block in HBCN.

```
Function verifyBlock(block, originalHash):
      Input: block, originalHash
      Output: true or false
      1.  calculatedHash <- hashBlock(block)
      2.  return calculatedHash == originalHash
End Function

Function verifyFort2BCKSignature(signature, publicKey, data):
      Input: signature, publicKey, data
      Output: true or false
1. return ECDSA.verify(publicKey, data, signature)  // Use
   ECDSA function to verify
End Function

Function addBlockToBlockchain(block):
      Input: block
      Output: none
      1.  blockchain.add(block)
End Function
```

Figure 8 Final verification of the mined block.

reflecting a 60% reduction in verification failure rate and an 18% reduction in computational cost, as detailed in Table 2.

4.3 Results and Analysis

4.3.1 Analysis of results: Security and performance

The results demonstrate that the integration of Fort2BCK into the healthcare blockchain network (HBCN) significantly optimises security and efficiency. Specifically, Scenario 3 (Fort2BCK with ECDSA and ZKP) showed the highest decrease in data tampering risk and the highest detection rate of data

Table 2 Comparison of security and performance between scenarios

Scenario	Handling Risk (%)	Detected Attacks (%)	Improving Detected Attacks	Average Latency (ms)	Average CPU Load (%)
HBCN Standard	12.3%	65%	–	150	45
Fort2BCK (ECDSA)	2.1%	92%	+27%	160	48
Fort2BCK (ECDSA + ZKP)	0.9%	98%	+33%	170	52

Table 3 Block validation time (ms)

Number of Blocks	Standard HBCN Validation (ms)	HBCN and Fort2BCK Validation (ms)	Improvement (%)
20	880	616	30%
40	1760	1232	30%
60	2640	1848	30%
80	3520	2464	30%
100	4400	3080	30%

integrity attacks, albeit with a marginal increase in latency. The following table compares the performance of three test scenarios: standard HBCN, Fort2BCK with ECDSA, and Fort2BCK with ECDSA and ZKP. The metrics evaluated include: reduction in data tampering risk (%), data integrity attack detection rate (%), increase in data integrity attack detection rate, average latency (ms), and average CPU load (%). The data indicates a substantial reduction in the risk of data tampering and a significant increase in the detection of data integrity attacks when implementing Fort2BCK, with a slight increase in latency and CPU load.

4.3.2 Latency analysis

As can be seen, the introduction of Fort2BCK, especially with ZKP, increases latency. This is due to the additional execution times for ECDSA signature generation (12 ms) and verification with ZKP. However, the increase in latency remains within operational limits for EHR applications, where accuracy and security are a priority.

Table 3 compares the block validation time between standard HBCN and HBCN with Fort2BCK for different numbers of blocks. The columns are: Number of blocks, standard HBCN validation (ms), HBCN + Fort2BCK validation (ms) and improvement (%). The data shows a consistent 30% reduction in validation time with Fort2BCK.

Validation time analysis: A 30% reduction in block validation time was achieved thanks to the implementation of Fort2BCK. The time was measured

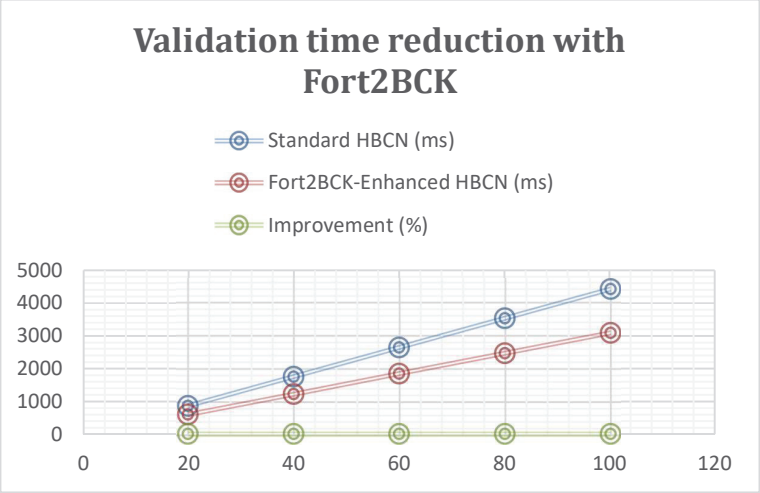


Figure 9 Validation time reduction with Fort2BCK.

from the time the block was generated until it was validated by the HBCN-B node. This analysis demonstrates that Fort2BCK reduces block validation time by approximately 30%, optimising the verification process without compromising security or decentralisation.

Figure 9 illustrates the impact of Fort2BCK on block validation time. The graph shows the validation time in milliseconds (Y-axis) as a function of the number of blocks processed (X-axis), comparing the standard healthcare blockchain network (HBCN) with the enhanced version incorporating Fort2BCK. The blue line represents the validation time for the standard HBCN, while the red line indicates the validation time for the enhanced HBCN with Fort2BCK. The green line shows the percentage improvement in validation time. A 30% reduction in validation time is consistently observed with Fort2BCK, demonstrating the optimised efficiency of the verification process without compromising safety and decentralisation.

4.3.3 Security evaluation

Table 3 shows a notable reduction in the risk of data manipulation and a substantial increase in the attack detection rate when implementing Fort2BCK. This result is attributed to the additional layer of cryptographic verification introduced by Fort2BCK, which validates each block before it is incorporated into the blockchain. The use of Schnorr's ECDSA digital signatures and zero knowledge proofs (ZKPs) establishes a robust guarantee of authenticity and

integrity, significantly decreasing vulnerability to attacks such as data forgery and replay attacks.

4.3.4 Discussion

The findings confirm the effectiveness of Fort2BCK as a robust and efficient security layer for healthcare blockchain networks (HBCNs). Dual validation and the use of cryptographic signatures optimise both security and data integrity, while the optimisation of redundant processes improves computational efficiency. The analysis of the mining process, detailed in Section 4.2, facilitates the understanding of the impact of the execution times of functions such as hashBlock and digital signature generation on the overall validation time. Despite the slight increase in CPU load due to cryptographic operations, the improvement in security and overall efficiency justifies this increase.

5 Conclusion

Fort2BCK emerges as an essential solution to strengthen security in blockchain infrastructures, especially in critical sectors such as healthcare. By integrating dual verification with digital signatures (ECDSA) and zero knowledge proofs (ZKPs), it significantly reduces the risk of data manipulation. Unlike other solutions, it operates independently of the consensus algorithm, which allows its adaptability to various blockchain networks and increases its resilience against attacks such as 51% and Sybil.

The results demonstrate substantial improvements in the efficiency and security of healthcare blockchain networks (HBCNs), including a 30% reduction in block validation time, a 60% decrease in verification failure rate and an 18% reduction in computational load, as well as facilitating regulatory compliance (HIPAA, GDPR). Fort2BCK, by actively preventing data manipulation, sets a new standard in blockchain infrastructure protection.

Future directions include evaluation in high-volume environments, optimisation of computational resources through algorithms such as BLS, integration with smart contracts and advanced privacy technologies such as zk-SNARKs and homomorphic encryption, as well as expansion into other critical sectors such as finance, government and supply chain.

In summary, Fort2BCK represents a significant advance in blockchain security, offering a scalable and efficient solution for protecting sensitive data and preventing fraud. Its adaptability and robustness position it as a crucial component for ensuring the integrity and reliability of future blockchain infrastructures in an ever-evolving cyber threat environment.

References

[1] K. Ramar, P. V. Gopirajan, H. Shanmugasundaram, B. P. Andraju, and S. Baskar, "Digital Healthcare using Blockchain," *2022 1st Int. Conf. Comput. Sci. Technol. ICCST 2022 – Proc.*, pp. 651–655, 2022, doi: 10.1109/ICCST55948.2022.10040411.

[2] A. Cervera García and A. Goussens, "Cybersecurity and use of ICT in the health sector," *Aten. Primaria*, vol. 56, no. 3, p. 102854, 2024, doi: 10.1016/j.aprim.2023.102854.

[3] A. M. Udroiu, M. Dumitrache, and I. Sandu, "Improving the cybersecurity of medical systems by applying the NIST framework," *2022 14th Int. Conf. Electron. Comput. Artif. Intell. ECAI 2022*, pp. 1–7, 2022, doi: 10.1109/ECAI54874.2022.9847498.

[4] Z. Baruwa, S. Bhattacherjee, S. R. Chandnani, and Z. Zhu, "Social Media Perceptions of 51% Attacks on Proof-of-Work Cryptocurrencies: A Natural Language Processing Approach," pp. 1–23, 2023, [Online]. Available: http://arxiv.org/abs/2310.14307.

[5] Y. Wang and M. Tan, "Defense against sybil attack in blockchain based on improved consensus algorithm," *2023 IEEE Int. Conf. Control. Electron. Comput. Technol. ICCECT 2023*, pp. 986–989, 2023, doi: 10.1109/ICCECT57938.2023.10140278.

[6] S. Yan, "Analysis on Blockchain Consensus Mechanism Based on Proof of Work and Proof of Stake," *Proc. – 2022 Int. Conf. Data Anal. Comput. Artif. Intell. ICDACAI 2022*, pp. 464–467, 2022, doi: 10.1109/ICDACAI57211.2022.00098.

[7] N. Ettaloui, S. Arezki, and T. Gadi, "An Overview of Blockchain-Based Electronic Health Record and Compliance with GDPR and HIPAA BT – Artificial Intelligence, Data Science and Applications," 2024, pp. 405–412.

[8] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," *Proc. – 2016 2nd Int. Conf. Open Big Data, OBD 2016*, pp. 25–30, 2016, doi: 10.1109/OBD.2016.11.

[9] K. Ito, K. Tago, and Q. Jin, "I-Blockchain: A Blockchain-Empowered Individual-Centric Framework for Privacy-Preserved Use of Personal Health Data," *Proc. – 9th Int. Conf. Inf. Technol. Med. Educ. ITME 2018*, pp. 829–833, 2018, doi: 10.1109/ITME.2018.00186.

[10] P. Verma, V. Tripathi, and B. Pant, "ZeroMedChain: Layer 2 Security and Zero-knowledge Proof Integration for Decentralized Identity

and Access Management in Healthcare," *Proc. 18th INDIAcom; 2024 11th Int. Conf. Comput. Conf. Comput. Glob. Dev. INDIACom 2024*, pp. 1023–1027, 2024, doi: 10.23919/INDIACom61295.2024.10498190.

[11] M. M. Nuttah, P. Roma, G. Lo Nigro, and G. Perrone, "Understanding blockchain applications in Industry 4.0: From information technology to manufacturing and operations management," *J. Ind. Inf. Integr.*, vol. 33, no. March, p. 100456, 2023, doi: 10.1016/j.jii.2023.100456.

[12] A. J, D. P. Isravel, K. M. Sagayam, B. Bhushan, Y. Sei, and J. Eunice, "Blockchain for healthcare systems: Architecture, security challenges, trends and future directions," *J. Netw. Comput. Appl.*, vol. 215, no. April, p. 103633, 2023, doi: 10.1016/j.jnca.2023.103633.

[13] S. Pandey, A. K. De, S. Choudhary, and M. Asim, "A Decentralized Blockchain-Based Architecture for Healthcare Industry," *Int. Conf. Artif. Intell. Innov. Healthc. Ind. ICAIIHI 2023*, vol. 1, pp. 1–5, 2023, doi: 10.1109/ICAIIHI57871.2023.10489491.

[14] M. Wang, T. Zhu, X. Zuo, D. Ye, S. Yu, and W. Zhou, "Public and Private Blockchain Infusion: A Novel Approach to Federated Learning," *IEEE Internet Things J.*, vol. 11, no. 10, pp. 17525–17537, 2024, doi: 10.1109/JIOT.2024.3360129.

[15] S. Baskar and P. V. Gopirajan, "Application of Blockchain in Digital Healthcare," *Proc. Int. Conf. Intell. Innov. Technol. Comput. Electr. Electron. ICIITCEE 2023*, pp. 591–595, 2023, doi: 10.1109/IITCEE57236.2023.10091070.

[16] M. J. H. Faruk, H. Shahriar, M. Valero, S. Sneha, S. I. Ahamed, and M. Rahman, "Towards Blockchain-Based Secure Data Management for Remote Patient Monitoring," *Proc. – 2021 IEEE Int. Conf. Digit. Heal. ICDH 2021*, pp. 299–308, 2021, doi: 10.1109/ICDH52753.2021.00054.

[17] M. A. Islam et al., "Distributed Ledger Technology Based Integrated Healthcare Solution for Bangladesh," *IEEE Access*, vol. 11, pp. 51527–51556, 2023, doi: 10.1109/ACCESS.2023.3279724.

[18] H. Guo, W. Li, M. Nejad, and C. C. Shen, "A Hybrid Blockchain-Edge Architecture for Electronic Health Record Management With Attribute-Based Cryptographic Mechanisms," *IEEE Trans. Netw. Serv. Manag.* vol. 20, no. 2, pp. 1759–1774, 2023, doi: 10.1109/TNSM.2022.3186006.

[19] S. Fahim, S. Katibur Rahman, and S. Mahmood, "Blockchain: A Comparative Study of Consensus Algorithms PoW, PoS, PoA, PoV," *Int. J. Math. Sci. Comput.*, vol. 9, no. 3, pp. 46–57, 2023, doi: 10.5815/ijmsc.2023.03.04.

[20] M. Jo, D. Kim, and S. Park, "Analysis of Byzantine Fault Tolerant Consensus Algorithms," *Int. Conf. Inf. Netw.*, pp. 205–207, 2024, doi: 10.1109/ICOIN59985.2024.10572154.

[21] H. Shriya, V. P. Marakumbi, N. Soumya, D. G. Narayan, H. Altaf, and S. Pooja, "An Efficient Voting Based Consensus Algorithm for Permissionless Blockchains," *2023 14th Int. Conf. Comput. Commun. Comput. Technol. ICCCNT 2023*, pp. 1–5, 2023, doi: 10.1109/ICCCNT 56998.2023.10307611.

[22] A. Abidi, B. Bouallegue, and F. Kahri, "Implementation of elliptic curve digital signature algorithm (ECDSA)," *GSCIT 2014 – Glob. Summit Comput. Inf. Technol.*, pp. 1–6, 2014, doi: 10.1109/GSCIT.2014.697 0118.

[23] A. Ali, B. A. A. S. Al-rimy, F. S. Alsubaei, A. A. A. Almazroi, and A. A. A. Almazroi, "HealthLock: Blockchain-Based Privacy Preservation Using Homomorphic Encryption in Internet of Things Healthcare Applications," *Sensors*, vol. 23, no. 15, pp. 1–29, 2023, doi: 10.3390/s2 3156762.

[24] O. Kuznetsov, A. Rusnak, A. Yezhov, D. Kanonik, K. Kuznetsova, and S. Karashchuk, "Enhanced Security and Efficiency in Blockchain with Aggregated Zero-Knowledge Proof Mechanisms," *IEEE Access*, vol. 12, no. March, pp. 49228–49248, 2024, doi: 10.1109/ACCESS.2024.3384 705.

[25] A. Jurevic Sokol, "Clinical Research and Data: HIPAA, the Common Rule, the General Data Protection Regulation, and Data Repositories," *Merrill Ser. Res. Mission Public Univ. Mission*, pp. 47–62, 2017, doi: 10.17161/merrill.2017.7750.

[26] C. J. Tinoco-Plasencia, "Blockchain Technology Applied in Medicine: a Systematic Review," *Rev. la Fac. Med. Humana* , vol. 24, no. 1, pp. 144–161, 2024, doi: 10.25176/RFMH.v24i1.5900.

[27] E. R. D. Villarreal, J. Garcia-Alonso, E. Moguel, and J. A. H. Alegria, "Blockchain for Healthcare Management Systems: A Survey on Interoperability and Security," *IEEE Access*, vol. 11, no. January, pp. 5629–5652, 2023, doi: 10.1109/ACCESS.2023.3236505.

[28] A. L. A. A. Fonsêca et al., "Blockchain in Health Information Systems: A Systematic Review," *Int. J. Environ. Res. Public Health*, vol. 21, no. 11, pp. 1–18, 2024, doi: 10.3390/ijerph21111512.

[29] C. M. Nalayini, Jeevaakatiravan, P. V. Imogen, and J. M. Sahana, "A Study on Digital Signature in Blockchain Technology," *Proc. 3rd Int.*

Conf. Artif. Intell. Smart Energy, ICAIS 2023, no. Icais, pp. 398–403, 2023, doi: 10.1109/ICAIS56108.2023.10073680.

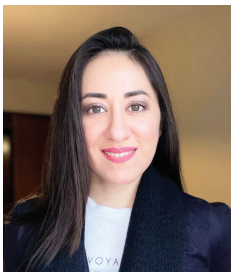
[30] D. Capko, S. Vukmirovic, and N. Nedic, "State of the Art of Zero-Knowledge Proofs in Blockchain," *2022 30th Telecommun. Forum, TELFOR 2022 – Proc.*, pp. 9–12, 2022, doi: 10.1109/TELFOR56187.2022.9983760.

[31] Y. K. Tomov et al., "Understanding blockchain applications in Industry 4.0: From information technology to manufacturing and operations management," *Inf. Process. Lett.*, vol. 2022-June, no. March, pp. 1–6, 2022, doi: 10.1109/EDUCON.2018.8363488.

Biographies

Cinthia Paola Pascual Caceres obtained a degree in Software Development Engineering in 2013 and a Master's degree in Cybersecurity from the University of Alicante in 2020. Currently, she is studying for a PhD in Computer Science at the University of Alicante. Her research interests include computing, Blockchain technology, networking and forensics. Helena has worked on projects that improve security and digital efficiency, exploring Blockchain applications and advancing forensic methodologies to combat cyber threats.

José Vicente Berná Martínez was born in Spain in 1978. He received his engineering degree and PhD degree in Computer Science from the University of Alicante in 2004 and 2011, respectively. From 2006 to 2013, he was an Associate Professor at the University of Alicante. Currently he is an Assistant doctor. His research interests are in the area of computer networks, distributed systems, bio-inspired systems and robotics that are applied to industrial problems.



María Esther Almaral Martínez was born in Mexico in 1989. She graduated with a degree in Software Development Engineering in 2012 and a master's degree from the University of Alicante in 2021. She is currently pursuing a PhD in Computer Science at the University of Alicante. She has research interests in computer science, UX/UI and digital security. She has been working on projects related to improving digital security as well as user interfaces and user experience, her goal is to find a balance between backend and frontend functionality.

Lucía Arnau Muñoz was born in Spain in 2000. She obtained her degree in Computer Engineering from the Universitat Politècnica de València in 2022, and an Official Master in Cybersecurity in 2023 from the University of Alicante, where she is currently a PhD student in Computer Science. In 2022 she started working as a Technical Specialist in the Smart University project, funded by Next Generation funds, as an expert in sensor networks and IoT systems. The research areas she is currently working on are distributed systems, advanced and scalable architectures, IoT and sensor networks.