International Journal on Optimization and Applications
IJOA. Vol. 4, Issue No. 2, Year 2024, www.ijoa.ma

Elliptic Curve Cryptography in Blockchain Technology: Challenges and Opportunities

1st Alaa BAHHOU
ENSAK
0009-0001-4699-3963

2nd Nohayla BELARBI
ENSAK
0009-0000-8522-9338

3th Khawla ELAHMADI
ENSAK
khawla.elahmadi@uit.ac.ma

4th Soukayna KERKAA
ENSAK
0009-0009-1433-8700

5th Ayoub LAMHAMDI
ENSAK
ayoub.lamhamdi@uit.ac.ma

***Abstract*—Elliptic Curve Cryptography (ECC) plays a critical role in ensuring data security within blockchain technology. This study delves into the challenges and opportunities surrounding the integration of ECC in blockchain networks. We begin by emphasizing the critical importance of data security in the digital age, highlighting the role of ECC in safeguarding sensitive information on blockchain platforms. We pose the central question: "How safe is your data on ECC's blockchain?" Moving forward, we provide an overview of ECC in blockchain security, defining both blockchain and ECC while elucidating ECC's significance in cryptographic applications within blockchain systems. Subsequently, we delve into the challenges faced by ECC-based blockchain networks. In light of these challenges, this study introduces HAE (hybrid AES and ECC), an innovative hybrid cryptographic algorithm that ingeniously combines the agility of AES with the robustness of ECC. HAE is designed to symmetrically encrypt original data with AES while employing ECC for the asymmetric encryption of the initial AES key. This strategy not only alleviates the complexities associated with AES key management but also enhances the algorithm's security without compromising its efficiency. Furthermore, we explore practical applications of ECC in blockchain technology, highlighting its potential to mitigate security risks and enhance trust during transactions. Additionally, we discuss advancements in ECC and blockchain security, emphasizing the ongoing efforts to improve data integrity and privacy within Blockchain-based systems. In conclusion, we advocate for the widespread adoption of ECC in blockchain technology as a means of securing financial data and preserving data integrity, paving the way for a more secure and transparent financial ecosystem.**

***Index Terms*—ECC, blockchain, HAE, Cryptography, security**

I. Introduction

In this ever-evolving world, there is a growing lean, particularly prominent in sectors such as finance, banking, smart contracts, or the voting system, towards a decentralized, secure, and transparent way to store and manage data. Blockchain technology, with its decentralized nature and tamper resistance, holds promise for addressing these concerns. Cryptographic algorithms, essential components of blockchain technology, offer solutions to challenges related to data volume, diversity, storage, and sharing.

As organizations and individuals increasingly rely on blockchain technology to store and manage sensitive information, understanding the intricacies of ECC's role in safeguarding this data becomes imperative. With its extensive adoption, particularly in blockchain networks, ECC (Elliptic Curve Cryptography) has become a foundation of modern cryptographic security. However, this widespread adoption raises a crucial question: How safe is your data on ECC's blockchain?

Answering this question will enlighten us on the complex synergy of challenges and opportunities that define a new perspective of data security in this digital age. ECC offers a robust pillar for encryption, authentication, and digital signatures, providing the backbone for secure transactions and data management in blockchain systems. Yet, it also confronts unique challenges in the face of evolving threats and technological advancements.

One such advancement is the Elliptic Curve Qu-Vanstone Implicit Certificate Scheme (ECQV), which presents new possibilities for key agreement in elliptic curve cryptography but is not commonly used. However, as with any emerging technology, there are both challenges and opportunities to be explored, particularly in the vast landscape of cryptography.

This article delves into the challenges and opportunities that ECC presents while ensuring the safety of data within blockchain systems. From addressing vulnerabilities posed by quantum computing and scalability, to exploring the opportunities that ECC's security paradigm provides.

This paper also discusses the advantage that the traditional cryptographic algorithms AES brings when implemented with ECC. AES offers rapid encryption and decryption capabilities but faces challenges in key management and distribution. ECC provides enhanced security with reduced key sizes and computational overhead, suitable for resource-limited environments. However, ECC may encounter efficiency challenges when processing large volumes of data.

To address these challenges, this article introduces a hybrid cryptographic algorithm that integrates the strengths of both AES and ECC. In this approach, AES encrypts the data swiftly, while ECC secures the AES key. This hybrid algorithm is applied to data storage and sharing in blockchain systems, with experimental analysis conducted to assess its security, time efficiency, resource consumption, and advantages. To apply HAE (hybrid AES and ECC) in the field of online education, this paper structures it as follows:

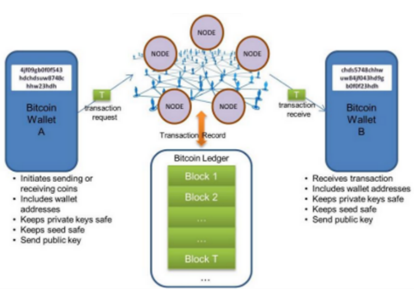
1) Data Encryption: Use AES for symmetric encryption of sensitive educational data. AES provides robust security and efficiency, making it suitable for data encryption.
2) Key Encryption: Employ ECC for asymmetric encryption of the AES key. ECC provides a smaller key size and faster computations, which is crucial for secure key management.
3) Secure Transmission: Share the encrypted data and the encrypted AES key between two educational institutions using a secure channel, such as a secure blockchain network.
4) Decryption: The receiving educational institution can use the shared AES key to decrypt the encrypted data, and the shared ECC key to decrypt the AES key. This allows them to access the original sensitive educational data securely.

By using the HAE hybrid cryptographic algorithm, educational institutions can ensure the security and integrity of sensitive educational data while addressing the challenges associated with managing AES keys. This approach can be applied to various fields, including online education, to securely transmit sensitive information between parties.

II. Overview of ECC in Blockchain Security

A. *Definition of blockchain*

A blockchain is a distributed database, also known as a specific type of a distributed ledger technology, shared among a computer network's nodes. It is best known for its crucial role in cryptocurrency systems for maintaining a secure and decentralized record of transactions. However, it is not limited to cryptocurrency uses. Blockchain can be used to make data in any industry unalterable.



1) Understanding Blocks in Blockchain: A blockchain forms a secure, interconnected chain of blocks, each holding a collection of transactions and vital data. Through cryptographic techniques, these blocks are intricately linked, ensuring the integrity and immutability of the entire ledger.

[1]

Blocks represent fundamental data structures within the blockchain database, responsible for permanently recording transactional data in a cryptocurrency blockchain. Each block encapsulates a portion of the most recent transactions awaiting validation by the network.

Following validation, the block concludes, paving the way for the creation of a fresh block to accommodate new transactions awaiting validation.

A block, therefore, serves as an unchangeable repository of records, impervious to alteration or deletion once inscribed.

Because there is no way to change a block, the only trust needed is at the point where a user or program enters data. This aspect reduces the need for trusted third parties, which are usually auditors or other humans that add costs and make mistakes.

2) Mechanics of a Block in Blockchain: Within a blockchain network, a flurry of transactional activities unfolds. In the realm of cryptocurrencies, maintaining a ledger of these transactions facilitates monitoring of expenditure and involved parties. These transactions, occurring over a specified duration, are encapsulated within a file termed a block, serving as the foundational unit of the blockchain network.

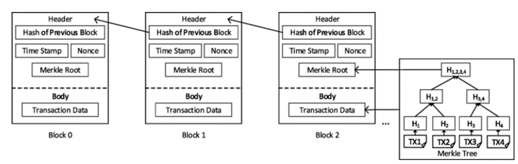


Fig. 1. Enter Caption
[2]

In the blockchain, each block is like a link in a chain, holding a unique stamp that ties it to the one before it. This stamp, known as the previous block's hash, acts as a digital fingerprint, ensuring the integrity and continuity of the blockchain.

Additionally, the very first block, known as the "Genesis Block," sets the foundation for the entire chain, kicking off the sequence without any previous block to reference. When it's time to add a new block to the chain, the blockchain community relies on consensus mechanisms like proof of work (PoW) or proof of stake (PoS) to collectively agree on its validity, maintaining the decentralized integrity of the network.

A block serves as a vessel for information. While diverse components populate a block, its storage footprint remains relatively modest. Typically, a block incorporates these following constituents:

1) **Header**: The header of a block contains metadata and crucial information about the block, including:
   - Block Number: A unique identifier for the block within the blockchain.
   - Timestamp: The time at which the block was created.
   - Previous Hash: The cryptographic hash of the previous block's header, creating the chain-like structure of the blockchain.

- Merkle Root: The cryptographic hash of all the transactions included in the block, ensuring the integrity of the transactions.
- Nonce: A random number used in the process of mining to satisfy the difficulty target of the blockchain network.

2) **Body (Transactions)**: The body of a block contains a list of transactions that are grouped together and added to the blockchain. Each transaction represents a transfer of value or data between participants in the blockchain network. The transactions include:
   - Sender and Receiver Addresses: The addresses of the sender and receiver involved in the transaction.
   - Amount: The amount of cryptocurrency or data being transferred.
   - Transaction ID: A unique identifier for each transaction.
   - Additional Data: Optional data fields that may include timestamps, signatures, or smart contract instructions.
3) **Hash**: The block's header, along with its transactions, is hashed using a cryptographic hashing algorithm such as SHA-256. This hash uniquely identifies the block and ensures its integrity. Any change to the block's contents will result in a completely different hash.
4) **Mining**: Mining is the process of creating new blocks and adding them to the blockchain. Miners compete to solve a cryptographic puzzle by finding a nonce that, when combined with the block's data, produces a hash that meets the difficulty target set by the blockchain network. Once a miner successfully mines a block, they broadcast it to the network for validation and inclusion in the blockchain.
5) **Validation**: Once a block is mined, it is broadcast to the network, where other nodes validate its contents and verify its authenticity. Nodes check that the transactions are valid, the block's hash meets the difficulty target, and the block follows the consensus rules of the blockchain network.
6) **Addition to the Blockchain**: Upon successful validation, the new block is added to the blockchain by linking its header to the previous block's hash. This creates a continuous and immutable chain of blocks, with each block containing a record of transactions that cannot be altered without altering subsequent blocks.

3) Exploring Mining's Role in Blocks: Mining constitutes the endeavor to resolve the nonce, essential in validating block headers within a cryptocurrency network, especially under proof-of-work protocols. Despite misconceptions about its complexity, mining primarily involves generating a random number via hashing—an encryption method integral to cryptocurrency operations. The arduous nature of solving the nonce highlights the energy-intensive nature of mining, reliant on a formidable network of miners and large energy reserves.

The intricate nature of block headers, compounded by encryption, emphasizes the formidable challenge posed by mining endeavors.

4) Clarifying Blockchain in Layman's Terms: In essence, a blockchain constitutes a secure database employing cryptographic techniques to interlink information, ensuring immutability while mandating network consensus for data validation.

III. ECC DEFINITION AND ITS SIGNIFICANCE IN BLOCKCHAIN CRYPTOGRAPHY

Elliptic-Curve Cryptography (ECC) is a type of public key cryptosystem that uses elliptic-curve theory to secure data. In public key cryptography, each user has a pair of keys – a public key and a private key. The public key can be freely shared with anyone, while the private key is kept secret. Data encrypted with the public key can only be decrypted with the corresponding private key.

Elliptic Curve Cryptography (ECC) plays a crucial role in enhancing blockchain security through its efficient and advanced cryptographic techniques. Unlike methods like RSA (Rivest–Shamir–Adleman), ECC offers several advantages that make it a preferred choice for secure public-key encryption within blockchain networks.

One significant advantage of ECC is its ability to achieve the same level of security as RSA but with significantly smaller key sizes. This not only reduces the computational overhead but also speeds up the encryption and decryption processes, which is essential for the seamless execution of blockchain transactions. (are transactions encrypted).

Elliptic Curve Cryptography (ECC) plays a crucial role in enhancing the security infrastructure of blockchain systems through its efficient and advanced cryptographic techniques. Unlike methods like RSA (Rivest–Shamir–Adleman), ECC offers several advantages that make it a preferred choice for secure public-key encryption within blockchain networks.

One significant advantage of ECC is its ability to achieve the same level of security as RSA but with significantly smaller key sizes. This not only reduces the computational overhead but also speeds up the encryption and decryption processes, which is essential for the seamless execution of blockchain transactions.

ECC's prowess in encryption is particularly noteworthy, as it enables the secure transmission of sensitive information across blockchain networks. By encrypting data using ECC-based algorithms, blockchain systems ensure that confidential information remains shielded from unauthorized access and tampering. Moreover, ECC's role in authentication is paramount in verifying the identities of participants within blockchain ecosystems.

Through the use of public-private key pairs generated by ECC, participants can authenticate themselves and sign transactions with their private keys, which can then be verified by others using their corresponding public keys. This mechanism not only ensures the authenticity of transactions but also reinforces trust and reliability within blockchain networks. Additionally, ECC's adoption of the Elliptic Curve Digital

Signature Algorithm (ECDSA) underscores its significance in facilitating secure digital signatures, which are fundamental for transaction verification and validation in blockchains.

The utilization of ECDSA enables blockchain systems to generate strong and reliable digital signatures, thereby fortifying the overall security posture of decentralized networks. Furthermore, ECC's widespread adoption across prominent blockchain platforms such as Bitcoin and Ethereum underscores its established reputation and efficacy in bolstering blockchain security. As blockchain technology continues to evolve and proliferate across various domains, ECC remains an indispensable tool for safeguarding data integrity, confidentiality, and authenticity in decentralized systems. Through its adept handling of encryption, authentication, and digital signatures, ECC stands as a stalwart guardian of blockchain security, ensuring the resilience and trustworthiness of distributed ledger technologies in the digital age.

IV. Challenges of Data Security on ECC's Blockchain

As demonstrated numerous times before, data has become the new-age currency. Thus, ensuring its safety and integrity has become a crucial stake for many. However, the security of blockchain systems heavily relies on the cryptographic techniques employed, with Elliptic Curve Cryptography (ECC) playing an essential role.

This section delves into the safety of data within blockchain networks, exploring the challenges faced by ECC-based implementations, particularly concerning scalability and quantum threats.

A. Safety of Data within Blockchain Networks

Blockchain networks are revered for their inherent security mechanisms, which make them resistant to tampering and unauthorized access. These networks achieve security through cryptographic techniques, decentralization, and consensus mechanisms.

Cryptography: Cryptography plays a central role in ensuring the safety of data within blockchain networks. Each block in the blockchain is cryptographically linked to the previous one, creating an immutable chain.

This immutability is achieved through several cryptographic techniques:

- **Cryptographic Hashing**: Each block contains a cryptographic hash of the previous block. When a block is added to the blockchain, its hash is included in the next block. If any data within a block is altered, the hash will change, making it easy to detect tampering.
- **Digital Signatures**: Transactions within blocks are secured through digital signatures. Digital signatures are created using a user's private key and can be verified using their public key. This ensures that the transaction was indeed initiated by the user who holds the private key, providing non-repudiation.
- **Public-Key Cryptography**: The use of public-key cryptography is essential for digital signatures. In this system, each user has a pair of keys: a public key and a private key. The public key is shared with others, while the private key is kept secret. When a user signs a transaction, they use their private key to generate a digital signature. Others can then use the user's public key to verify the signature's authenticity.
- **Symmetric Key Encryption**: While digital signatures provide non-repudiation, symmetric key encryption is used to protect the actual transaction data within a block. AES (Advanced Encryption Standard) is a commonly used symmetric encryption algorithm that provides robust security and efficiency.
- **Key Management**: ECC (Elliptic Curve Cryptography) is used for key management in blockchain networks. ECC provides a smaller key size and faster computations, which is crucial for secure key management in a decentralized system like blockchain.

Decentralization: Blockchain networks operate in a decentralized manner, meaning that there is no single point of control or failure. This decentralization enhances the security of the network by distributing trust among multiple participants (nodes) rather than relying on a central authority.

Consensus Mechanisms: Consensus mechanisms such as proof of work (PoW) or proof of stake (PoS) ensure that all participants in the network agree on the validity of transactions and the order in which they are added to the blockchain. By achieving consensus, blockchain networks prevent double-spending and other malicious activities.

- **Proof of Work (PoW)**: is the original consensus algorithm in a blockchain network. In this system, miners compete to solve a complex mathematical problem, which requires significant computational power. Once a miner solves the problem, they are rewarded with a new block and the transaction fees associated with the block. This process is energy-intensive and requires a high level of computational power, making it difficult for a single entity to control the network.
- **Proof of Stake (PoS)**: is an alternative consensus mechanism that uses a different approach. In PoS, validators are chosen based on the amount of cryptocurrency they hold, referred to as their stake. Validators are responsible for appending transactions to the blockchain and are rewarded for doing so. To prevent a single entity from gaining control over the network, PoS requires that validators have a significant stake in the cryptocurrency. This mechanism is more energy-efficient than PoW but requires a different set of security measures to ensure the integrity of the network.

B. Challenges Faced by ECC-Based Implementations

While elliptic curve cryptography (ECC) is widely used in blockchain networks for its efficiency and security, it also presents certain challenges, particularly concerning scalability and quantum threats.

Scalability:

As blockchain networks continue to evolve and witness a surge in transactional throughput, scalability emerges as a pressing concern. ECC, while offering significant advantages in terms of computational efficiency and key sizes, confronts scalability challenges due to its reliance on complex mathematical operations. ECC's computational overhead increases with the size of the network and the volume of transactions processed. The elliptic curve-based algorithms used for key generation, digital signatures, and encryption demand substantial computational resources, potentially impeding the scalability of blockchain networks, or leading to potential bottlenecks particularly in high-throughput environments.

For ECC-based blockchain implementations like Bitcoin and Ethereum, as the network grows, the sheer volume of transactions and the increasing number of users strain the network's capacity, resulting in congestion, higher transaction costs, and slower transaction speeds. These scalability issues are exacerbated by the growing number of nodes in the network, as each node must process and validate all transactions to maintain the integrity of the blockchain.

At a technical level, scalability concerns arise primarily from the limitations of the underlying consensus mechanisms and the architecture of the blockchain network. For example, Bitcoin's proof-of-work (PoW) consensus algorithm requires miners to solve complex mathematical puzzles to validate transactions and add new blocks to the blockchain. However, as the network grows, the computational resources required to solve these puzzles increase exponentially, leading to longer confirmation times and higher transaction fees.

Quantum Threats:

The introduction of quantum computing poses a significant threat to traditional cryptographic schemes, including ECC. Quantum computers leverage principles of quantum mechanics to perform computations at an unprecedented speed, potentially rendering conventional cryptographic algorithms vulnerable to attacks. ECC, although currently considered secure against classical adversaries, is susceptible to quantum attacks due to its reliance on the discrete logarithm problem over elliptic curves for security. Thus, quantum resistance is a critical concern for ECC-based blockchain implementations, as current cryptographic algorithms like ECDH and ECDSA are vulnerable to attacks by quantum computers.

One of the most notable quantum algorithms that threatens ECC-based cryptography is Shor's algorithm. Shor's algorithm efficiently factors large integers, which forms the basis of many cryptographic algorithms used in blockchain protocols. By factoring large integers, Shor's algorithm can break the underlying mathematical assumptions of ECC-based encryption schemes, compromising the confidentiality and integrity of blockchain transactions.

V. Opportunities for Enhancing Data Security

A. Countermeasures and Post-Quantum Cryptography

In response to these challenges, the field of cryptography is actively exploring post-quantum cryptographic algorithms that are believed to be secure against quantum computing attacks. These include lattice-based cryptography, hash-based cryptography, and multivariate polynomial cryptography, among others. Incorporating these quantum-resistant algorithms into blockchain frameworks represents a proactive approach to safeguarding against future quantum threats.

The transition to post-quantum cryptography, however, introduces its own set of challenges, including the need for increased computational resources and potential impacts on transaction speeds and blockchain scalability.

The blockchain community, therefore, faces the dual challenge of enhancing cryptographic security while maintaining or improving performance metrics critical to user experience and adoption.

In this paragraph, we will introduce some solutions for the challenges presented above to answer the scalability and quantum threats, as well as introduce a hybrid encryption method of ECC with a fast and secure algorithm, which is the AES-256 encryption algorithm, in the next section.

1) Scalability: To address scalability challenges in ECC-based blockchain implementations, there are various solutions:

Layer-2 solutions represent a paradigm shift in blockchain scalability, offering a nuanced approach to alleviating the burden on the main blockchain while enhancing transaction throughput and cost efficiency.

The Lightning Network is a layer 2 protocol designed to facilitate off-chain transactions on the Bitcoin blockchain. It operates using a network of payment channels, which are essentially smart contracts that enable participants to transact with each other directly, without involving the main blockchain for every transaction.

Benefits of Layer 2 Solutions:

- **Scalability**: Layer 2 solutions offer a scalable approach to processing transactions, allowing blockchain networks to handle a higher volume of transactions without experiencing congestion or delays.
- **Cost Efficiency**: Off-chain transactions in layer 2 solutions are often faster and cheaper than on-chain transactions, as they bypass the need for expensive consensus mechanisms and blockchain validation.
- **Decentralization**: Despite conducting transactions off-chain, layer 2 solutions maintain the decentralization and security properties of the underlying blockchain, ensuring that participants retain control over their funds and transactions.
- **Interoperability**: Layer 2 solutions can be interoperable with multiple blockchains, enabling seamless transactions and data exchange across different blockchain networks.
- **Layer 2 Solutions**: One approach is to implement layer 2 solutions that offload some transaction processing from the main blockchain. Examples include the Lightning Network for Bitcoin and sharding in Ethereum 2.0. These solutions enable faster and more cost-effective transactions by conducting most transactions off-chain and settling them on-chain periodically. By reducing the burden on the main blockchain, layer 2 solutions

International Journal on Optimization and Applications
IJOA. Vol. 4, Issue No. 2, Year 2024, www.ijoa.ma

can significantly improve scalability without sacrificing security or decentralization.

- **Optimized Consensus Mechanisms**: Another approach is to introduce new consensus mechanisms that are more efficient than PoW. Proof of Stake (PoS) is one such alternative consensus mechanism that selects validators based on the amount of cryptocurrency they hold and are willing to "stake" as collateral. By eliminating the need for energy-intensive mining, PoS can reduce the environmental impact of blockchain networks and improve scalability by increasing transaction throughput.

2) Quantum resistance: To address the quantum resistance challenge in ECC-based blockchain implementations, we explore the development and implementation of post-quantum cryptographic algorithms. Post-quantum cryptography aims to replace vulnerable cryptographic algorithms like ECC with quantum-resistant alternatives that remain secure even in the presence of quantum computers.

One of the primary concerns regarding the quantum threat to cryptographic systems, including those based on Elliptic Curve Cryptography (ECC), is the potential speedup of certain algorithms on quantum computers. Quantum computers have the potential to perform certain calculations significantly faster than classical computers due to their exploitation of quantum mechanical phenomena such as superposition and entanglement.

In the context of ECC and other public-key cryptography algorithms, the most prominent quantum algorithm of concern is Shor's algorithm. Shor's algorithm, developed by mathematician Peter Shor in 1994, demonstrates that a sufficiently powerful quantum computer could efficiently factor large integers and solve the discrete logarithm problem. These mathematical problems form the basis of many cryptographic schemes, including the RSA and ECC algorithms used for digital signatures, public-key encryption, and key exchange protocols.

In ECC, for instance, the security of the system relies on the difficulty of solving the elliptic curve discrete logarithm problem (ECDLP), which involves finding the discrete logarithm of a point on an elliptic curve. Currently, the best known classical algorithms for solving the ECDLP have exponential time complexity, making ECC secure against attacks using classical computers.

However, Shor's algorithm, when implemented on a sufficiently powerful quantum computer, could efficiently solve the ECDLP and compromise the security of ECC-based cryptographic systems. This represents a significant threat to the confidentiality, integrity, and authenticity of data stored and transmitted using ECC.

The speedup provided by quantum computers in solving these mathematical problems undermines the security assumptions underlying many cryptographic protocols. As a result, there is a pressing need to develop and adopt quantum-resistant cryptographic techniques that can withstand attacks from quantum adversaries.

The transition to post-quantum cryptography, however, introduces its own set of challenges, including the need for increased computational resources and potential impacts on transaction speeds and blockchain scalability.

The blockchain community, therefore, faces the dual challenge of enhancing cryptographic security while maintaining or improving performance metrics critical to user experience and adoption.

In the next section, we will introduce a new coupling method of ECC with a fast and secure algorithm, which is the AES encryption algorithm.

VI. Practical Application of HAE in Blockchain

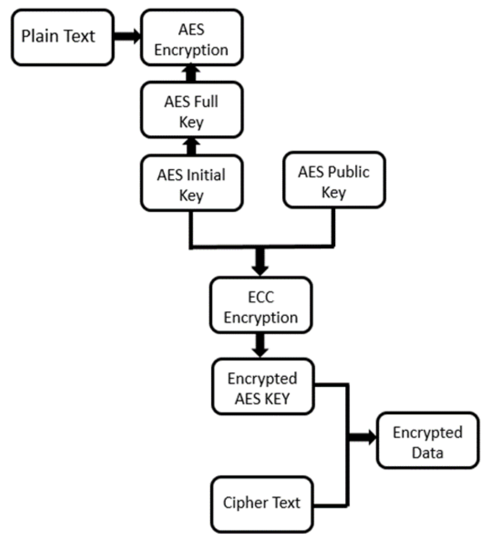


Fig. 2. Hybrid encryption of HAE

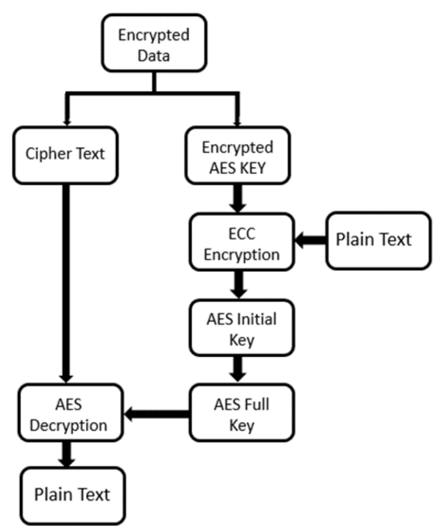


Fig. 3. Hybrid decryption of HAE

Integrating a hybridization of Elliptic Curve Cryptography (ECC) and the Advanced Encryption Standard (AES-256) within blockchain networks birth a pretty robust system that could be used in medical, financial or any other field. And here is how it can be done :

AES Key Generation:

- A 256-bit random number serves as the foundation for the AES initial key. This key is generated using cryptographic algorithms to ensure randomness and unpredictability.
- Through subsequent key expansion and alignment operations, the AES full key is derived from the initial key. Key expansion involves transforming the initial key into a larger set of round keys, while alignment ensures compatibility with AES encryption algorithms.
- The AES key generation process is crucial for establishing a secure encryption scheme, as the strength and randomness of the key directly impact the security of the encrypted data.

Plaintext Encryption:

- With the AES full key in hand, the plaintext data undergoes AES encryption, transforming it into ciphertext. AES encryption operates on fixed-size blocks of plaintext, typically 128 bits, making it suitable for encrypting extensive data like medical records.
- AES encryption involves a series of substitution, permutation, and mixing operations (known as rounds) applied to each plaintext block, ensuring a high level of security against cryptographic attacks.

AES Key Encryption:

- In this step, the AES initial key, generated in the first stage, is encrypted using the recipient's ECC public key. This encryption process enhances security by ensuring that only the intended recipient can decrypt the AES key.
- Encrypting only the AES initial key, rather than the entire AES full key, is a strategic decision aimed at increasing the difficulty for potential attackers attempting to intercept the key during transmission.

Encrypted Data Formation:

- The encrypted AES key and the ciphertext are combined to form the final encrypted data. This amalgamation ensures that both the encrypted key and the ciphertext are bundled together for transmission to the recipient.
- By packaging the encrypted AES key alongside the ciphertext, the integrity and confidentiality of the data are preserved during transmission, mitigating the risk of unauthorized access or tampering.

HAE Decryption Process:

- Upon receiving the encrypted data, the recipient first extracts both the ciphertext and the encrypted AES key from the received message.
- The ECC private key, possessed only by the recipient, decrypts the encrypted AES key, revealing the original AES initial key.
- The AES initial key then undergoes key expansion and alignment operations to reconstruct the AES full key.
- Finally, the AES full key is used to decrypt the ciphertext, reverting it back to the original plaintext data.

A. Benefits of HAE in Blockchain Security

The implementation of Hybrid Asymmetric Encryption (HAE) in a financial blockchain network offers several key benefits:

Enhanced Security: HAE combines the robustness of AES symmetric encryption with the cryptographic strength of ECC asymmetric encryption, providing strong security against unauthorized access and data breaches. The hybrid approach ensures that sensitive financial data remains confidential and tamper-proof, fostering trust and reliability among network participants.

Quantum-Resistant Key Management: With the looming threat of quantum computing, HAE offers quantum-resistant key management capabilities by leveraging ECC's resilience to quantum attacks. The use of ECC for key generation and encryption ensures that cryptographic keys remain secure even in the face of emerging quantum threats, safeguarding the integrity of blockchain transactions and data.

Efficiency and Performance: From a technical standpoint, a research paper has examined the CPU usage for the hybrid cryptographic algorithm HAE, and the results show a slight uptick as the amount of data increases, as shown in the figure below. However, in real-world scenarios like storing medical data in the InterPlanetary File System (IPFS), the hash address generated by IPFS doesn't require much storage space. Therefore, the resource consumption remains minimal. This suggests that HAE could be a valuable addition to blockchain applications in various fields, offering promising prospects for deployment without significant resource overhead.

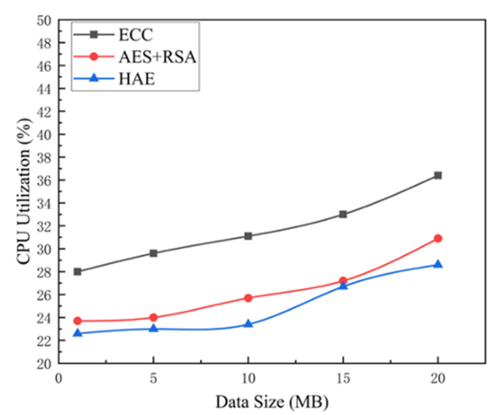


Fig. 4. Comparison of CPU utilization of three cryptographic algorithms. [3]

VII. Conclusion

In this study, we've delved into the crucial role of Elliptic Curve Cryptography (ECC) in ensuring the security of data within blockchain technology. From the outset, we've emphasized the paramount importance of data security in our digital era, underscoring ECC's pivotal role in safeguarding sensitive information on blockchain platforms. Our exploration began with a comprehensive overview of ECC in blockchain security, defining both blockchain and ECC while highlighting ECC's significance in cryptographic applications within blockchain systems.

Throughout our investigation, we've encountered various challenges faced by ECC-based blockchain networks, prompting us to introduce HAE (hybrid AES and ECC) as an innovative solution. HAE ingeniously combines the agility of AES with the robustness of ECC, offering a strategic approach to symmetrically encrypt original data with AES while employing ECC for asymmetric encryption of the initial AES key. This integration not only streamlines AES key management complexities but also enhances the algorithm's security without compromising its efficiency.

Furthermore, we've explored practical applications of ECC in blockchain technology, showcasing its potential to mitigate security risks and foster trust during transactions. Our discussion also touched upon the advancements in ECC and blockchain security, highlighting ongoing efforts to enhance data integrity and privacy within Blockchain-based systems.

In conclusion, we advocate for the widespread adoption of ECC in blockchain technology as a fundamental means of securing financial data and preserving data integrity. By embracing ECC, and using it as a leverage for other strong and fast cryptographic algorithms, we can pave the way for a more secure and transparent financial ecosystem, bolstering confidence in our digital transactions and fortifying the foundation of our digital age.

References

[1] Shiksha Online *Structure of a Block in Blockchain*2023
[2] Shiksha Online *Structure of a Block in Blockchain*2023
[3] Chen, Z., Gu, J., and Yan, H. *HAE: A Hybrid Cryptographic Algorithm for Blockchain Medical Scenario Applications* Appl. Sci, 2023.