Unlocking Potential: Leveraging Proof of Mobile for Blockchain Security

By

NOW Blockchain Team

Abstract:

In the landscape of blockchain technology, security remains a paramount concern. As traditional consensus mechanisms struggle to meet the demands of scalability and resistance to attacks, innovative solutions are imperative. This whitepaper introduces the NOW blockchain, a groundbreaking approach that leverages Proof of Mobile (PoM) function as a node to enhance security. By integrating mobile devices into the consensus mechanism, NOW blockchain offers a novel method to fortify the network against malicious actors while also promoting inclusivity and decentralization. This paper outlines the core concepts behind NOW blockchain, explores its technical architecture, and discusses the potential implications and benefits for the broader blockchain ecosystem.

Introduction:

The rapid evolution of blockchain technology has ushered in a new era of decentralized systems, promising unparalleled security, transparency, and trust. However, as blockchain networks continue to expand in scale and scope, traditional consensus mechanisms face inherent limitations that threaten their efficacy and resilience (Marr, 2023).

In response to these challenges, we introduce the NOW blockchain—a pioneering framework that redefines the conventional notion of consensus by integrating mobile devices into the network infrastructure. At its core, NOW blockchain leverages Proof of Mobile (PoM) as a novel consensus mechanism, harnessing the computational power and ubiquity of mobile devices to enhance security and decentralization.

The premise of PoM is rooted in the widespread adoption of smartphones and other mobile devices, which have become indispensable tools in our daily lives. According to forecasts, the global number of smartphone users is expected to continuously increase between 2024 and 2029 by a total of 1.5 billion users, representing a remarkable 30.6 percent growth (Statista, n.d.). After the fifteenth consecutive increasing year, the smartphone user base is estimated to

reach 6.4 billion users, marking a new peak in 2029 (Statista, n.d.). By harnessing the computational capabilities of these devices, NOW blockchain establishes a resilient network where every participant contributes to the consensus process, thereby mitigating the risks associated with centralized control and traditional mining algorithms.

This whitepaper proposes an in-depth exploration of the NOW blockchain, elucidating its technical underpinnings, architectural design, and potential impact on the broader blockchain ecosystem. Through a comprehensive analysis of PoM and its implications, we aim to demonstrate the transformative potential of NOW blockchain in addressing the pressing security challenges facing contemporary blockchain networks.

The Interplay of Security and Consensus in Decentralized Blockchain Networks

In the realm of decentralized blockchain technology, the concepts of security and consensus are inexorably intertwined, forming the bedrock upon which the entire ecosystem operates. At its core, a blockchain is a distributed ledger maintained by a network of nodes, each of which independently verifies and records transactions. The decentralized nature of this network is pivotal to its security and consensus mechanisms, which work in tandem to ensure the integrity and immutability of the ledger.

Security in the context of blockchain refers to the protection of the network against malicious actors and unauthorized access. In a centralized system, security often relies on a trusted authority to safeguard sensitive data and validate transactions. However, in a decentralized blockchain, there is no central authority; instead, security is achieved through cryptographic techniques and consensus protocols.

Consensus, on the other hand, refers to the process by which network participants agree on the validity of transactions and the state of the ledger. In a decentralized blockchain, achieving consensus among potentially adversarial nodes is crucial for maintaining the integrity of the ledger and preventing double-spending or other forms of fraud. Consensus mechanisms vary across different blockchain platforms, with each designed to balance factors such as security, scalability, and decentralization.

One of the most well-known consensus mechanisms is Proof of Work (PoW), which underpins the security of Bitcoin and several other cryptocurrencies. In a PoW system, network nodes, known as miners, compete to solve complex mathematical puzzles in order to validate

transactions and add new blocks to the blockchain. The first miner to solve the puzzle is rewarded with newly minted coins and the right to append the block to the ledger. This process not only secures the network against attacks but also ensures consensus among honest nodes by incentivizing them to follow the protocol.

However, PoW has faced criticism for its energy-intensive nature and susceptibility to centralization as mining becomes dominated by a few powerful entities. In response, alternative consensus mechanisms have emerged, each with its own approach to balancing security and decentralization.

Proof of Stake (PoS) is one such alternative that aims to address the drawbacks of PoW. In a PoS system, validators are chosen to create new blocks based on the amount of cryptocurrency they hold and are willing to "stake" as collateral. Validators are incentivized to act honestly, as they stand to lose their staked funds if they validate fraudulent transactions. PoS is often lauded for its energy efficiency and potential for greater decentralization, although it also introduces new challenges such as the "nothing-at-stake" problem and the risk of stake centralization.

Other consensus mechanisms, such as Delegated Proof of Stake (DPoS), Practical Byzantine Fault Tolerance (PBFT), and Directed Acyclic Graphs (DAGs), offer different approaches to achieving consensus in decentralized networks. Each mechanism has its own trade-offs in terms of security, scalability, and decentralization, and the choice of consensus algorithm often depends on the specific use case and goals of the blockchain project (Yue 2016).

Regardless of the consensus mechanism employed, security remains paramount in decentralized blockchain networks. Without robust security measures in place, the integrity of the ledger is compromised, leading to loss of trust among network participants and undermining the entire ecosystem. Consensus mechanisms play a vital role in ensuring that all nodes agree on the state of the ledger, thereby maintaining the network's security and enabling it to function as intended.

Security and consensus are fundamental pillars of decentralized blockchain technology, working hand in hand to safeguard the integrity of the ledger and ensure the trustworthiness of the network. By leveraging cryptographic techniques and consensus protocols, blockchain platforms can achieve a level of security and decentralization that is unparalleled by traditional centralized systems, laying the groundwork for a new era of trustless digital transactions and decentralized applications.

What are Consensus Mechanisms?

Consensus mechanisms are pivotal components within blockchain networks, serving as the foundational mechanism for achieving agreement and validation of transactions across decentralized systems. These mechanisms are essential for maintaining the integrity, security, and reliability of blockchain networks by ensuring that all participating nodes reach a mutual agreement on the validity of transactions and the state of the ledger.

One of the primary functions of consensus mechanisms is to resolve the issue of trust in decentralized environments where multiple, potentially adversarial parties are involved. By establishing a shared consensus protocol, blockchain networks can achieve distributed trust without relying on a central authority. This decentralized trust model is crucial for fostering transparency and eliminating the need for intermediaries in transactions.

Consensus mechanisms contribute significantly to scalability, transaction time, and security within blockchain networks. Regarding scalability, consensus algorithms determine how efficiently a blockchain network can process transactions and grow in size while maintaining performance. Some consensus mechanisms, such as Proof of Work (PoW), may face scalability challenges due to the intensive computational resources required for mining blocks. Conversely, other mechanisms like Proof of Stake (PoS) or Delegated Proof of Stake (DPoS) offer improved scalability by reducing the computational overhead associated with block validation (Liljeqvist, 2022).

Transaction time, or throughput, refers to the speed at which transactions can be processed and confirmed within a blockchain network. Consensus mechanisms directly impact transaction time by influencing the speed at which new blocks are created and added to the blockchain. For instance, PoW-based blockchains typically have longer block confirmation times compared to PoS-based blockchains, where block generation occurs more rapidly.

Moreover, consensus mechanisms are intricately linked to the security of blockchain networks. By requiring nodes to reach a consensus agreement before adding new transactions to the ledger, these mechanisms prevent malicious actors from tampering with the transaction history or executing double-spending attacks. Robust consensus algorithms help maintain the immutability and integrity of the blockchain, ensuring that past transactions cannot be altered without the consensus of the majority of network participants (Mansa, 2023).

Consensus mechanisms serve as the backbone of blockchain technology, facilitating agreement among decentralized nodes and enabling the secure, reliable, and efficient operation of blockchain networks. Through their role in scalability, transaction time, and security, consensus mechanisms play a vital role in shaping the performance and functionality of blockchain systems.

Ensuring Trust: The Crucial Role of Security in Blockchain Technology

Blockchain technology has rapidly emerged as a pioneering application model, amalgamating consensus mechanisms, distributed data storage, digital encryption technology, peer-to-peer transmission, and other computing paradigms. This amalgamation has yielded an effective platform for secure and decentralized information exchange. Central to this technology are digital encryption technologies, which constitute the cornerstone of blockchain cryptography. Iredale (2021) underscores the importance of security in blockchain, emphasizing its role in fostering user trust and facilitating the widespread adoption of blockchain technology. Indeed, blockchain's distributed database architecture, characterized by decentralization, security, traceability, reliability, and immutability, obviates the need for traditional centralized data management approaches. Furthermore, it enables mutual node maintenance by multiple users, ensuring information supervision by diverse parties while upholding data integrity and credibility. Iredale's exposition also delineates the three primary types of blockchain platforms—public chain, private chain, and alliance chain—each offering distinct features and functionalities catering to diverse organizational needs and regulatory requirements. Despite its initial association primarily with the financial sector, blockchain technology exhibits significant potential for transformative impact across various industries, heralding a paradigm shift in societal norms and operational frameworks (Iredale, 2021). As such, an in-depth understanding of blockchain cryptography is indispensable for navigating the intricacies of this groundbreaking technology landscape.

What is Blockchain Security?

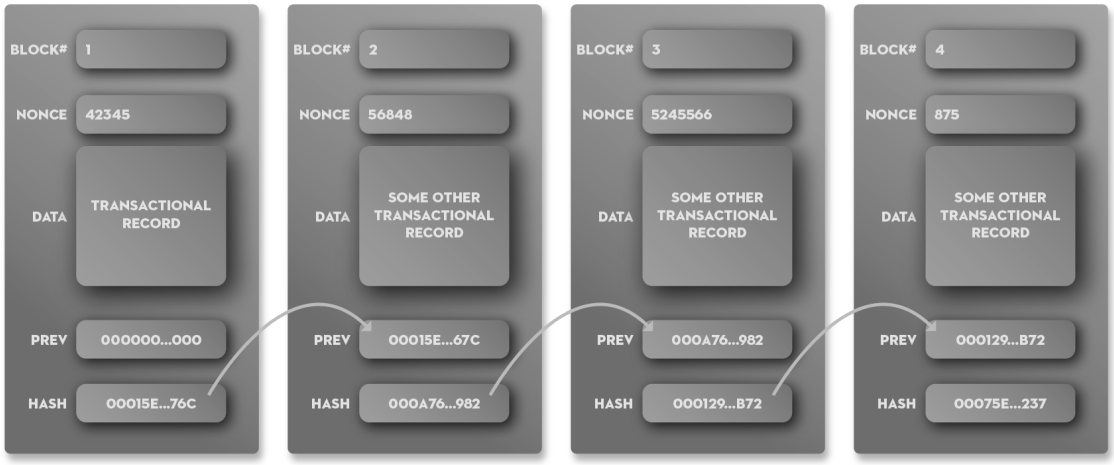
Blockchain technology, rooted in cryptography, decentralization, and consensus mechanisms, establishes a secure framework for data integrity and transactional trust. This architecture,

characterized by the organization of data into immutable blocks, interconnected through cryptographic hashing, forms the bedrock of blockchain security. Each transaction, encapsulated within these blocks, undergoes validation and consensus agreement, safeguarding the accuracy and authenticity of the recorded information. While blockchain technology inherently mitigates risks associated with centralized systems, variations in implementation introduce nuances in security considerations. For an in-depth exploration of basic blockchain security principles and best practices, consult IBM's resources on blockchain security (IBM, n.d.).

Types of Cryptography in Blockchain

Cryptography serves as the cornerstone of security within the realm of blockchain technology, providing a robust mechanism for safeguarding data from unauthorized access and manipulation. In essence, it forms the bedrock upon which the trust and integrity of blockchain transactions are established. Within the blockchain ecosystem, cryptography assumes a pivotal role in securing transactions occurring between various nodes dispersed across the network. As elucidated by Shobhit Seth in a piece dated May 15, 2022, published on Investopedia, cryptography operates in tandem with hashing, the other fundamental concept in blockchain technology. While hashing is primarily responsible for securing block information and the interlinking of blocks, cryptography focuses on encrypting messages within the peer-to-peer (P2P) network.

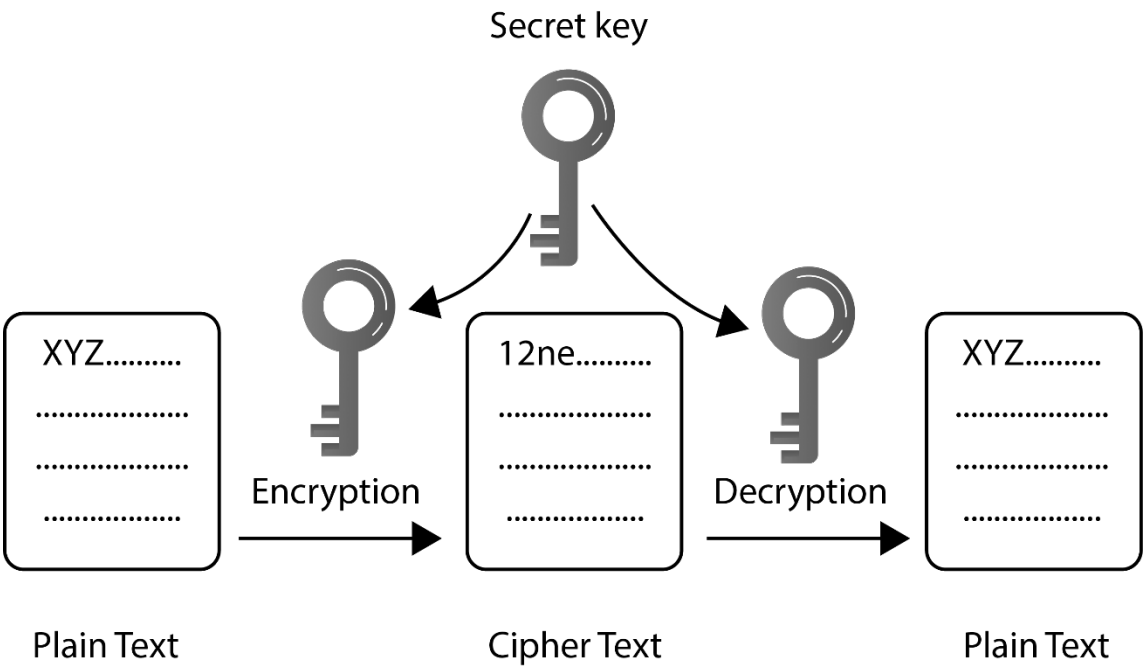
The utilization of cryptography within blockchain networks encompasses a range of cryptographic techniques, including symmetric encryption and asymmetric encryption. Symmetric encryption, as outlined by Seth, involves the use of a single key for both encryption and decryption processes, ensuring that the encrypted data can only be accessed and deciphered by parties possessing the corresponding key. On the other hand, asymmetric encryption, also referred to as public-key cryptography, employs a pair of distinct keys – a public key and a private key – with the former disseminated openly while the latter remains confidential. This approach, elucidated by Jasra Bhat in a publication dated August 2021 on ResearchGate, ensures that data encrypted with a public key can only be decrypted by the corresponding private key, thereby bolstering the security of transactions within the blockchain network.



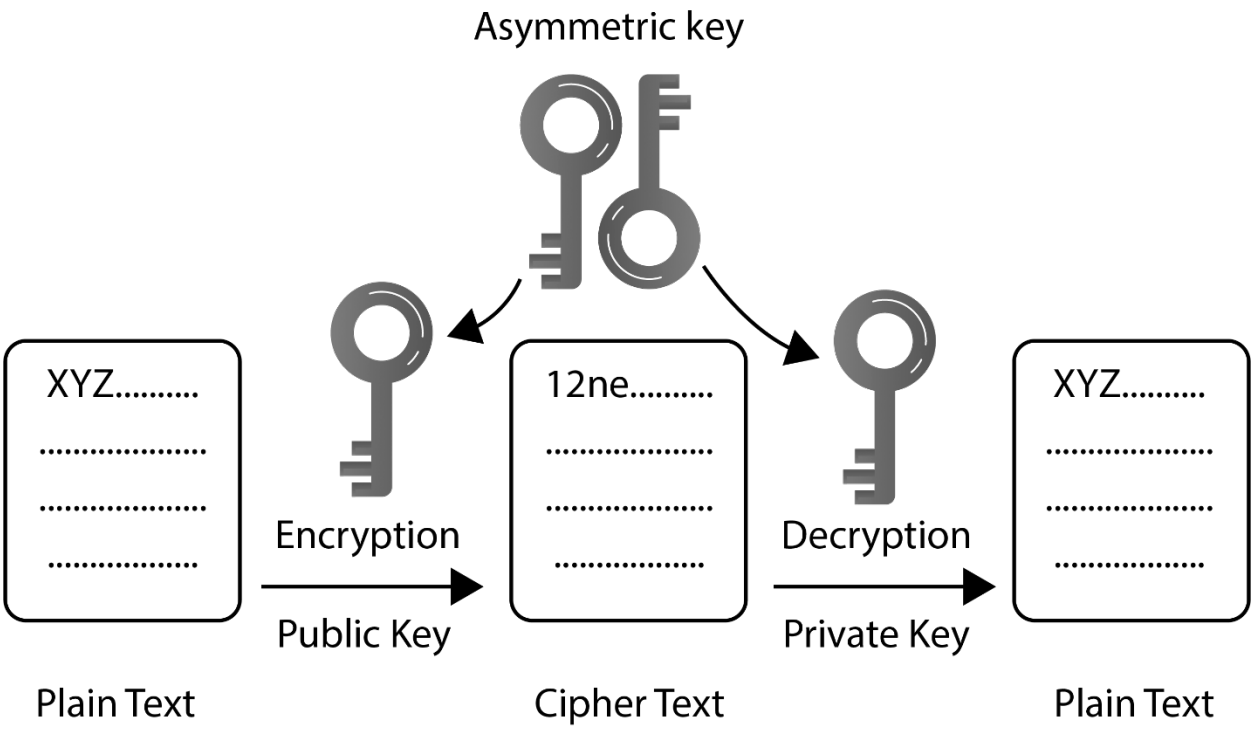
The overarching objective of cryptography within the blockchain ecosystem is to fortify the security of participants, transactions, and mitigate the risk of double-spending – a nefarious practice wherein a digital currency holder illicitly spends the same funds more than once. Through the implementation of cryptographic protocols, blockchain networks enforce stringent measures to authenticate the validity of transactions and ascertain the integrity of data exchanges. By encrypting transaction data, cryptography ensures that only intended recipients possess the requisite authorization to access, interpret, and process the underlying information, thereby safeguarding the confidentiality and integrity of sensitive data transmitted across the network.

Furthermore, cryptography within blockchain technology serves as a linchpin in establishing and maintaining the immutability of transaction records. Through the utilization of cryptographic hashing functions, such as SHA-256 (Secure Hash Algorithm 256-bit), blockchain networks generate unique digital signatures – commonly referred to as cryptographic hashes – for each block containing transaction data. These hashes serve as immutable fingerprints, intricately linked to the contents of the corresponding block, thereby facilitating the verification and validation of transactional integrity. Any alteration to the data within a block would invariably result in a modification of its cryptographic hash, thereby alerting network participants to the presence of tampering attempts and preserving the integrity of the blockchain ledger.

Moreover, cryptography plays a pivotal role in the consensus mechanisms employed by blockchain networks to facilitate agreement among distributed nodes regarding the validity of transactions and the subsequent addition of blocks to the blockchain. Consensus algorithms, such as Proof of Work (PoW) and Proof of Stake (PoS), leverage cryptographic principles to authenticate the computational efforts expended by network participants in validating transactions and appending new blocks to the blockchain. Through the integration of cryptographic puzzles and cryptographic signatures within consensus protocols, blockchain networks ensure the verifiability and integrity of transactional data, thereby fostering trust and consensus among disparate network nodes.



Symmetric encryption (Fig 1)



Asymmetric encryption (Fig 2)

Exploring Which Advanced Asymmetric Encryption Methods for Modern Digital Security

In an era defined by rapid technological advancement and digital connectivity, ensuring the security of sensitive information is paramount. NOW Blockchain team is dedicated to pioneering solutions in digital security, seeks to delve into the intricacies of advanced asymmetric encryption methods. Asymmetric encryption, also known as public-key encryption, stands as a cornerstone in safeguarding data transmission and communication integrity across open networks. NOW Blockchain team aims to explore each method, including Diffie-Hellman, RSA, ECDSA, ElGamal, and DSA, alongside the most recent and advanced technique of Elliptic Curve Cryptography (ECC). These encryption techniques not only bolster the security of open communication networks but also enable the seamless integration of confirmed identities into the Modern Digital Era (MDE). By analyzing the latest insights and advancements from scholarly articles and expert perspectives, NOW Blockchain team endeavors to shed light on the efficacy, strengths, and applications of these encryption methods in today's dynamic digital landscape.

Asymmetric Encryption Methods:

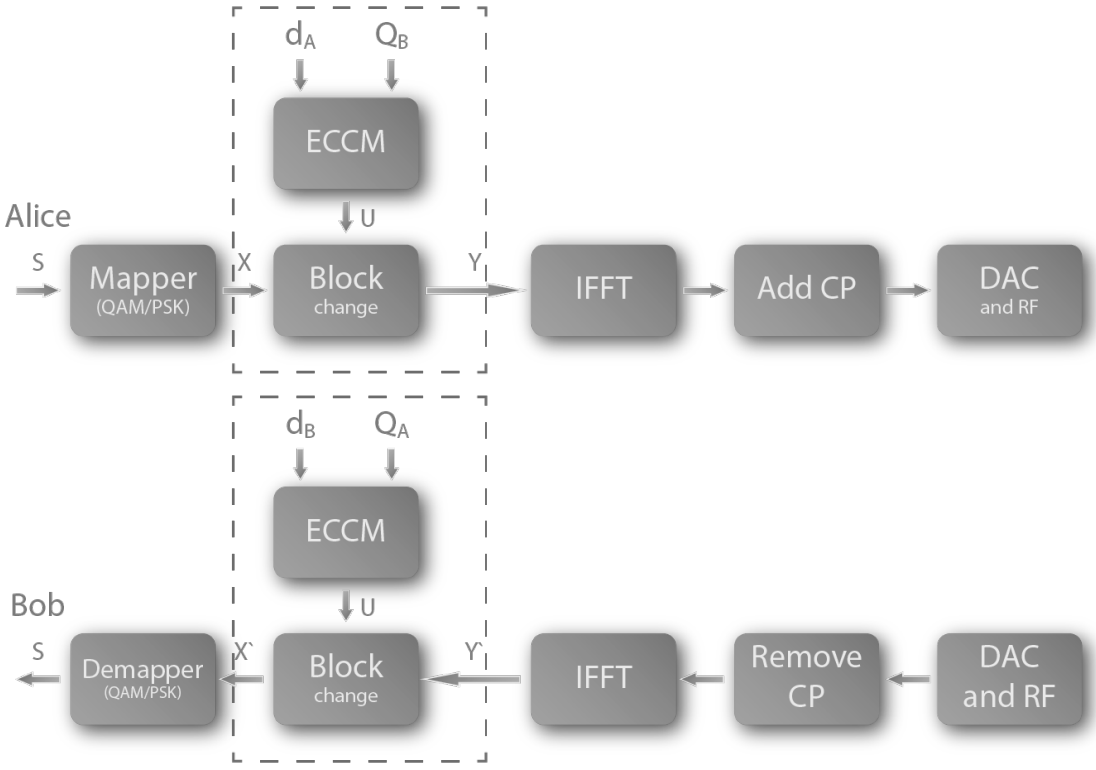
1. **Diffie-Hellman (DH):** Diffie-Hellman key exchange protocol facilitates secure communication by enabling parties to establish a shared secret over an insecure channel. Its security relies on the computational difficulty of solving the discrete logarithm problem, making it resilient against eavesdropping attacks. DH serves as a fundamental component in various cryptographic protocols, including TLS and SSH.
2. **RSA (Rivest-Shamir-Adleman):** RSA remains one of the most widely used asymmetric encryption algorithms, with its security based on the difficulty of factoring large prime numbers. It offers flexibility in key size, ranging from 1024 to 4096 bits, allowing for adaptation to diverse security requirements. Despite its longevity, RSA continues to be a cornerstone of modern encryption.
3. **Elliptic Curve Digital Signature Algorithm (ECDSA):** ECDSA is a variant of the Digital Signature Algorithm (DSA) based on elliptic curve cryptography. It offers comparable security to RSA but with smaller key sizes, making it particularly suitable for resource-constrained environments. ECDSA's efficiency and robust cryptographic operations contribute to its widespread adoption in modern cryptographic systems.
4. **ElGamal Encryption:** ElGamal encryption, derived from the Diffie-Hellman key exchange protocol, provides semantic security against chosen ciphertext attacks. Although less prevalent than RSA and ECDSA, ElGamal encryption finds applications in secure messaging systems and digital signatures.
5. **DSA (Digital Signature Algorithm):** DSA provides digital signatures for authentication purposes, ensuring data integrity and non-repudiation. It is standardized by organizations such as the National Institute of Standards and Technology (NIST) and is often used in conjunction with symmetric encryption algorithms.
6. **Elliptic Curve Cryptography (ECC):** ECC represents the most recent and advanced technique in asymmetric encryption, offering enhanced security with smaller key sizes compared to traditional methods. ECC is particularly suited for securing open communication networks and enabling secure access for individuals with confirmed identities into the Modern Digital Era (MDE) (Ullah et al. 2023).

Understanding the most common attacks on blockchain security

Some of the most common attacks on blockchain security, as outlined by Muhammad Yousuf Munir (January 1, 2023), include 51% attacks, double-spending attacks, man-in-the-middle attacks, DDoS attacks, and smart contract vulnerabilities. A 51% attack occurs when a single entity gains control of over 50% of the network's hashing power, allowing them to manipulate transactions and potentially double-spend coins. Double-spending attacks involve spending the same cryptocurrency tokens more than once by exploiting vulnerabilities in the blockchain's consensus mechanism. Man-in-the-middle attacks target the communication between nodes in a blockchain network, allowing attackers to intercept and manipulate data transmissions. Distributed Denial of Service (DDoS) attacks aim to disrupt blockchain network operations by overwhelming nodes with a flood of malicious traffic. Smart contract vulnerabilities can be exploited to execute unauthorized transactions or access sensitive data stored on the blockchain. Understanding and preventing these common attacks are crucial for maintaining the security and integrity of blockchain networks.

Enhancing Security with Elliptic Curve Cryptography in NOW Blockchain: A Strategic Approach

In the ever-evolving landscape of cybersecurity, the importance of robust encryption methods cannot be overstated. As technological advancements continue to proliferate across industries, ensuring the security of sensitive data becomes paramount. NOW Blockchain, a prominent player in the field of digital security solutions, has recognized the significance of leveraging cutting-edge cryptographic techniques to fortify its offerings. In this analytical paper, we delve into the strategic decision of NOW Blockchain to focus on employing Elliptic Curve Cryptography (ECC) within a binary field, particularly in conjunction with International Mobile Equipment Identity (IMEI), to elevate security standards (Abdurahmonov et al, 2011).



Understanding the Significance of ECC in Digital Security

Elliptic Curve Cryptography has gained widespread recognition and adoption owing to its superior security properties and efficiency compared to traditional cryptographic algorithms such as RSA. The mathematical underpinnings of ECC rely on the discrete logarithm problem, which is significantly harder to crack compared to factoring large prime numbers, the basis of RSA encryption. This inherent complexity makes ECC an appealing choice for securing digital communications and transactions.

One of the key advantages of ECC lies in its ability to provide equivalent security with shorter key lengths compared to RSA. This translates to reduced computational overhead and bandwidth requirements, making ECC particularly well-suited for resource-constrained environments such as mobile devices. Additionally, ECC offers robustness against quantum computing threats, positioning it as a future-proof cryptographic solution.

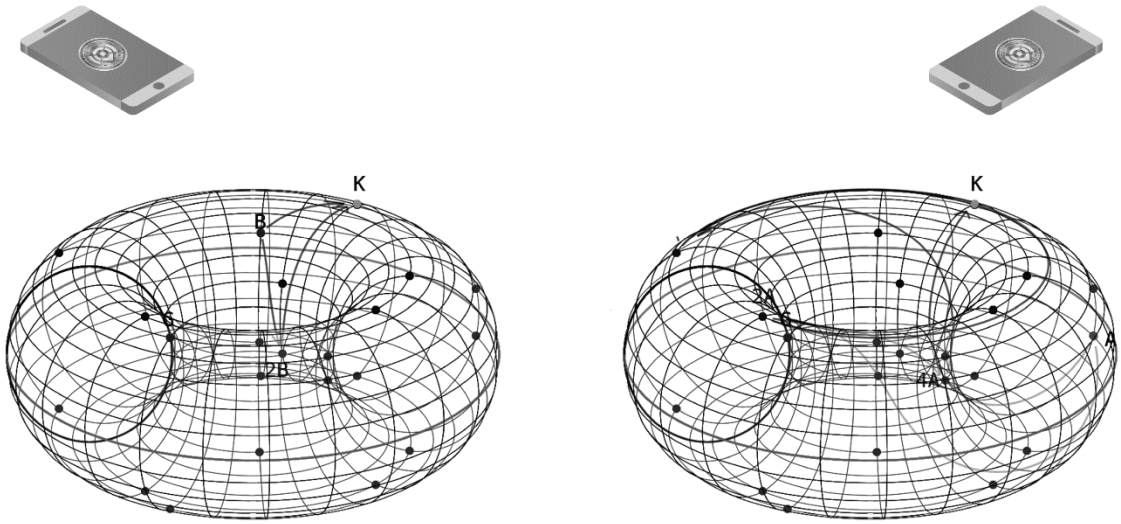
The Role of Binary Field in ECC Implementation

In ECC, the choice of field significantly impacts the efficiency and security of cryptographic operations. Traditionally, ECC is implemented over finite fields of prime order (prime fields) or binary fields. While both options offer comparable security, binary fields provide certain advantages in terms of implementation simplicity and computational efficiency.

By utilizing a binary field, NOW Blockchain can streamline the implementation of ECC algorithms, thereby reducing development time and minimizing the risk of implementation errors. Moreover, binary field arithmetic lends itself well to hardware acceleration techniques, enabling high-performance ECC implementations that are particularly well-suited for mobile and embedded systems.

Elliptic Curve Cryptography (ECC) in NOW Blockchain: A Comprehensive Analysis

In modern cryptography, Elliptic Curve Cryptography (ECC) stands as a pillar of secure communication and transaction protocols. The mathematical foundation of ECC revolves around the properties of elliptic curves over finite fields, offering robust encryption and digital signature schemes. This analytical paper not only delves into the fundamental principles of ECC but also explores its practical application within the NOW Blockchain ecosystem, elucidating its significance in contemporary cryptographic practices.



Fundamentals of Elliptic Curve Cryptography

Elliptic Curve Cryptography harnesses the algebraic properties of elliptic curves defined by equations of the form $Y^2 = x^3$+*ax*+*b*, where *a* and *b* are constants. These curves form an additive abelian group, with all coordinate points satisfying the curve equation. The addition operation on elliptic curves is well-defined, mimicking the reflection of the x-axis through intersecting points. ECC operates within finite fields *Fp*, ensuring that all algebraic operations remain within the confines of the field (Dhor 2022).

ECC in NOW Blockchain

NOW Blockchain integrates ECC as a fundamental component of its security infrastructure. By leveraging ECC, NOW Blockchain ensures the confidentiality, integrity, and authenticity of transactions within its decentralized network. ECC's efficient key generation and management mechanisms make it particularly well-suited for the resource-constrained environment of blockchain systems.

In NOW Blockchain, ECC plays a pivotal role in the following aspects:

1. **Secure Transaction Signing**: ECC facilitates the generation and verification of digital signatures, ensuring the authenticity and integrity of transactions recorded on the blockchain. Each transaction is signed using ECC-based cryptographic algorithms, providing robust protection against tampering and unauthorized modifications.
2. **Key Exchange Mechanisms**: ECC's efficiency in key generation and exchange makes it instrumental in establishing secure communication channels between network participants. NOW Blockchain utilizes ECC-based key exchange protocols to facilitate secure peer-to-peer communication and data transmission.
3. **Identity Management**: ECC enables the creation and management of digital identities within NOW Blockchain. Each user is assigned a unique public-private key pair based on ECC, allowing for secure authentication and access control within the decentralized network.
4. **Consensus Protocol Security**: ECC contributes to the security of NOW Blockchain's consensus protocol, ensuring the integrity of the distributed ledger and preventing malicious actors from tampering with the blockchain's transaction history.

In the context of Bitcoin and many other cryptographic implementations, the parameters x=0*a*=0 and Y=7*b*=7 are commonly utilized, simplifying the equation to Y^2=x^3+7Y^2=x^3+7.

The set of all coordinate points on an elliptic curve forms an additive abelian group, denoted as ∈ *E*.

The addition operation on elliptic curves is well-defined, where the sum of two points a=(a1,a2)*P*=(*p*1,*p*2) and b=(b1,b2)*Q*=(*q*1,*q*2) results in a third point on the curve. This addition operation mimics the reflection of the x-axis through the point where the line joining ∈ *P* and ∈ *Q* intersects the curve. Multiplication of a point by an integer ∈ *m* is achieved by adding the point to itself ∈ *m* times.

Elliptic Curve Cryptography in Finite Fields

ECC operates within a finite field *Fp*, where *p* is a prime number. All algebraic operations, including additions and multiplications of points on the elliptic curve, yield another point on the same curve. These operations are performed modulo *p*, ensuring that computations remain within the finite field (Dhor 2022)

The core components of ECC include the elliptic curve itself, a generator point *G* (a fixed base point on the curve), a private key *k*, and a corresponding public key *P*=*k*·*G*. The calculation of the public key from the private key, known as scalar multiplication, can be efficiently performed using algorithms like the "double-and-add algorithm," with a time complexity logarithmic in the magnitude of *k*.

Digital Signature Verification with ECDSA

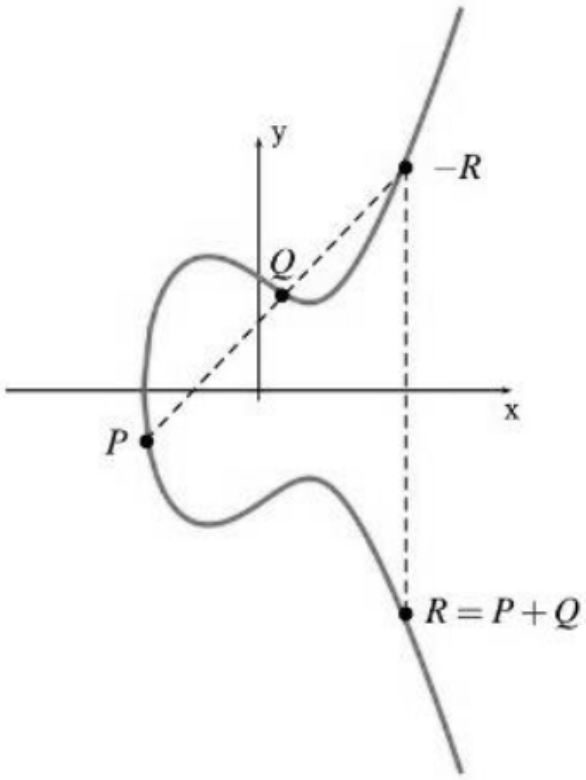
Elliptic Curve Digital Signature Algorithm (ECDSA) provides a secure method for generating and verifying digital signatures. To create a signature for a message *msg* using a private key *PrivKey*, the following steps are executed:

1. Compute the hash of the message, denoted as *h*=hash(*msg*).

2. Generate a random number *k* securely within the range [1,*n*], where *n* is the order of the generator point *G*.
3. Compute the point $R=k \cdot G$ and extract its x-coordinate *r*.
4. Calculate the signature component $s=k^{-1} \cdot (h+r \cdot \text{PrivKey}) \pmod{n}$.
5. The signature comprises the pair {*r*,*s*}.

To verify an ECDSA signature, the signed message along with the signature {*r*,*s*} and the corresponding public key *PubKey* are used. The verification process involves the following steps:

1. Compute the hash of the message: $h=\text{hash}(msg)$.
2. Reconstruct the point $'R'$ using the signature components: $R'=(h \cdot s-1) \cdot G+(r \cdot s-1) \cdot \text{PubKey}$.
3. Extract the x-coordinate $'r'$ from $'R'$.
4. Validate the signature by comparing whether $r'==r$.



Enhancing Security with Elliptic Curve Cryptography: A Closer Look at Curve Security Strength in NOW Blockchain

Elliptic Curve Cryptography (ECC) has garnered significant attention for its robust security properties and efficient cryptographic operations. One crucial aspect of ECC is its security strength, which is closely tied to the size of the elliptic curve used for cryptographic operations. This analysis delves into the intricacies of curve security strength in ECC and its implications for achieving desired levels of cryptographic security.

The security strength of an elliptic curve is determined by its ability to resist attacks, particularly against the Elliptic Curve Discrete Logarithm Problem (ECDLP). The fastest known algorithm to solve the ECDLP for a key size k requires approximately $2k$ steps. Therefore, to achieve a k-bit security strength, an elliptic curve with at least a $2k$-bit size is necessary.

For instance, 256-bit elliptic curves, where the field size p is a 256-bit number, typically provide nearly 128-bit security strength. However, it's essential to note that the actual security strength may be slightly less due to several factors. Firstly, the order of the curve (n) is often less than the field size (p). Additionally, the curve may have a cofactor ($\hbar h$) greater than 1, resulting in a subgroup order ($r=n/h$) smaller than n. Finally, the number of steps required for solving the ECDLP is not precisely $2k$, but approximately $0.886\times 2k$.

A precise estimation of security strength for popular standard elliptic curves can be found in reputable sources such as the SafeCurves project (http://safecurves.cr.yp.to/rho.html). For example, the secp256k1 curve (with $p=256$) provides approximately 128-bit security (more precisely, 127.8 bits), while the Curve448 curve (with $p=448$) offers roughly 224-bit security (around 222.8 bits).

Understanding the security strength of elliptic curves is essential for selecting appropriate curves that meet the desired level of security for cryptographic applications. Asymmetric key ciphers, particularly ECC, continue to play a crucial role in modern cryptography, and a thorough understanding of curve security strength enhances the overall security posture of cryptographic systems.

Applications of ECC

A notable application of ECC lies within the realm of blockchain technology, where it serves as the backbone for ensuring the security and integrity of transactions. In blockchain networks, ECC is utilized to generate public and private key pairs, which are integral to user authentication, data encryption, and digital signatures. By leveraging ECC, blockchain platforms can achieve a high level of security without compromising on performance or scalability.

One illustrative example of ECC in action within the blockchain domain is the Elliptic Curve Diffie-Hellman (ECDH) protocol. ECDH is a key exchange protocol that enables two parties to establish a shared secret over an insecure channel, thereby facilitating secure communication. The protocol leverages the properties of elliptic curves to achieve key agreement without the need for transmitting the actual keys over the network, thus mitigating the risk of interception by malicious entities.

Geeks for Geeks provides an insightful coding example demonstrating the implementation of the Elliptic Curve Diffie-Hellman Protocol, showcasing the practical application of ECC in real-world scenarios. Through this example, developers can gain a deeper understanding of how ECC can be integrated into their applications to enhance security and privacy.

Example of Elliptic curve Diffie-Hellman Protocol practice and followed according Geeks for Geeks written in Python.

Input

```
[2] pip install tinyec

    Looking in indexes: https://pypi.org/simple, https://us-python.pkg.dev/colab-wheels/public/simple/
    Collecting tinyec
      Downloading tinyec-0.4.0.tar.gz (24 kB)
    Building wheels for collected packages: tinyec
      Building wheel for tinyec (setup.py) ... done
      Created wheel for tinyec: filename=tinyec-0.4.0-py3-none-any.whl size=20892 sha256=168061ca46bf2820ce326230b9cd49756fef1dd578b78bb87ba7376ba8466de4
      Stored in directory: /root/.cache/pip/wheels/8e/5c/09/6730b2b261b8329cf6c339003a415b98ae1cdd1552d5882fcf
    Successfully built tinyec
    Installing collected packages: tinyec
    Successfully installed tinyec-0.4.0
```

```
# Importing required libraries used
# to perform arithmetic operations
# on elliptic curves
from tinyec import registry
import secrets

# Function to calculate compress point
# of elliptic curves
def compress(publicKey):
 return hex(publicKey.x) + hex(publicKey.y % 2)[2:]

# The elliptic curve which is used for the ECDH calculations
curve = registry.get_curve('brainpoolP256r1')

# Generation of secret key and public key
Ka = secrets.randbelow(curve.field.n)
X = Ka * curve.g
print("X:", compress(X))
Kb = secrets.randbelow(curve.field.n)
Y = Kb * curve.g
print("Y:", compress(Y))
print("Currently exchange the publickey (e.g. through Internet)")

# (A_SharedKey): represents user A
# (B_SharedKey): represents user B
A_SharedKey = Ka * Y
print("A shared key :",compress(A_SharedKey))
B_SharedKey = Kb * X
print("(B) shared key :",compress(B_SharedKey))
print("Equal shared keys:", A_SharedKey == B_SharedKey)
```

Output

```
from tinyec import registry
import secrets

def compress(publicKey):
 return hex(publicKey.x) + hex(publicKey.y % 2)[2:]

curve = registry.get_curve('brainpoolP256r1')
Ka = secrets.randbelow(curve.field.n)
X = Ka * curve.g
print("X:", compress(X))
Kb = secrets.randbelow(curve.field.n)
Y = Kb * curve.g
print("Y:", compress(Y))
print("Currently exchange the publickey (e.g. through Internet)")
#(A): represents person A
#(B): represents person B
A_SharedKey = Ka * Y
print("Person A shared key :",compress(A_SharedKey))
B_SharedKey = Kb * X
print("Person B shared key :",compress(B_SharedKey))
print("Whether shared keys are equal:", A_SharedKey == B_SharedKey)
```

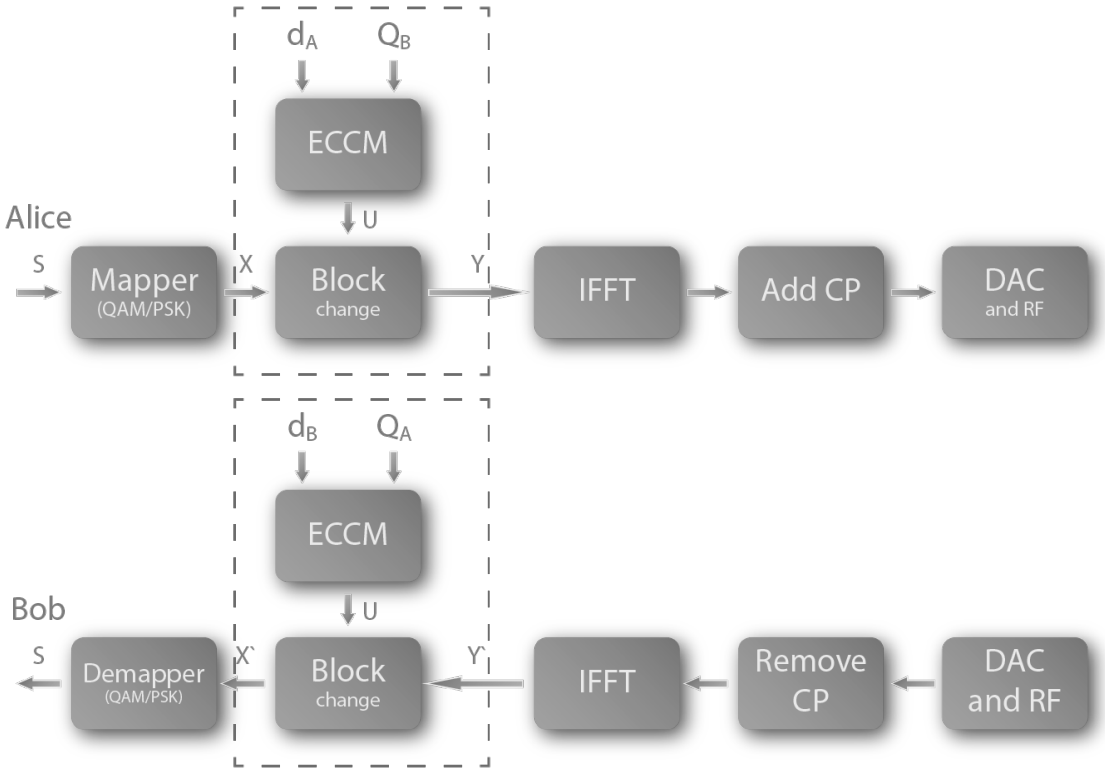
```
X: 0x24a00fe479b09b7a2117bc5d800d0491068e216b4eb172738f91dd9690d7e74d0
Y: 0x5bc45a276989a685af69d39d49ab8ce3492a73ac65a921958bf8db22b28e3bd91
Currently exchange the publickey (e.g. through Internet)
Person A shared key : 0x8bc97592d3d342cfd30633b3556c7b182ba92aaa781091c7117c7238aab02c101
Person B shared key : 0x8bc97592d3d342cfd30633b3556c7b182ba92aaa781091c7117c7238aab02c101
Whether shared keys are equal: True
```

Exploration and Exposition of Security Methods in NOW Blockchain

The Python code provided above serves as an illustrative example of the intricacies involved in generating an ECC (Elliptic Curve Cryptography) private-public key pair, particularly tailored for the recipient within a cryptographic communication system. This process is crucial in establishing a secure and confidential channel for transmitting sensitive information across blockchain networks. The code specifically operates on the brainpoolP256r1 elliptic curve, which is widely recognized for its robustness and computational efficiency, ensuring that cryptographic operations are performed with the utmost reliability and security.

In essence, the code follows a series of sequential steps to achieve its objectives. Initially, it initiates the generation of an ECC private-public key pair tailored specifically for the intended recipient. This key pair serves as the cornerstone of cryptographic operations, ensuring that communications remain confidential and resistant to unauthorized access. By exploiting the mathematical properties inherent in elliptic curves, the code produces a private key, known only to the recipient, and a corresponding public key, which can be freely shared with other parties involved in the communication process.

Subsequently, the code proceeds to derive two pivotal components: a secret shared key for encryption purposes and an ephemeral ciphertext key for facilitating Elliptic Curve Diffie-Hellman (ECDH) key exchange. This step is fundamental in establishing a secure communication channel, wherein both parties can securely exchange information without fear of interception or eavesdropping. By utilizing the recipient's public key, the code computes the shared secret key and ephemeral ciphertext key, thereby laying the groundwork for robust encryption and decryption mechanisms.



Furthermore, the code implements an integrated encryption scheme by utilizing the generated keys for both data encryption and decryption. This comprehensive approach ensures that sensitive information remains confidential during transit, thereby safeguarding against potential security breaches or data compromises. Notably, the code incorporates a randomized approach to generate the ciphertext private key, thereby enhancing the security of the encryption process and mitigating the risk of cryptographic attacks.

It is crucial to emphasize that the encryption and decryption keys derived from the ECC key pair remain consistent across multiple executions of the code, thereby ensuring interoperability and consistency in cryptographic operations. This stability underscores the reliability and resilience of the ECC-based encryption scheme, making it well-suited for a wide range of applications requiring secure communication channels within blockchain networks.

In the context of blockchain security, numerous considerations are taken into account when building and testing security features to ensure the integrity and confidentiality of transactions and data. These considerations encompass various aspects, including cryptographic protocols, consensus mechanisms, network architecture, and regulatory compliance.

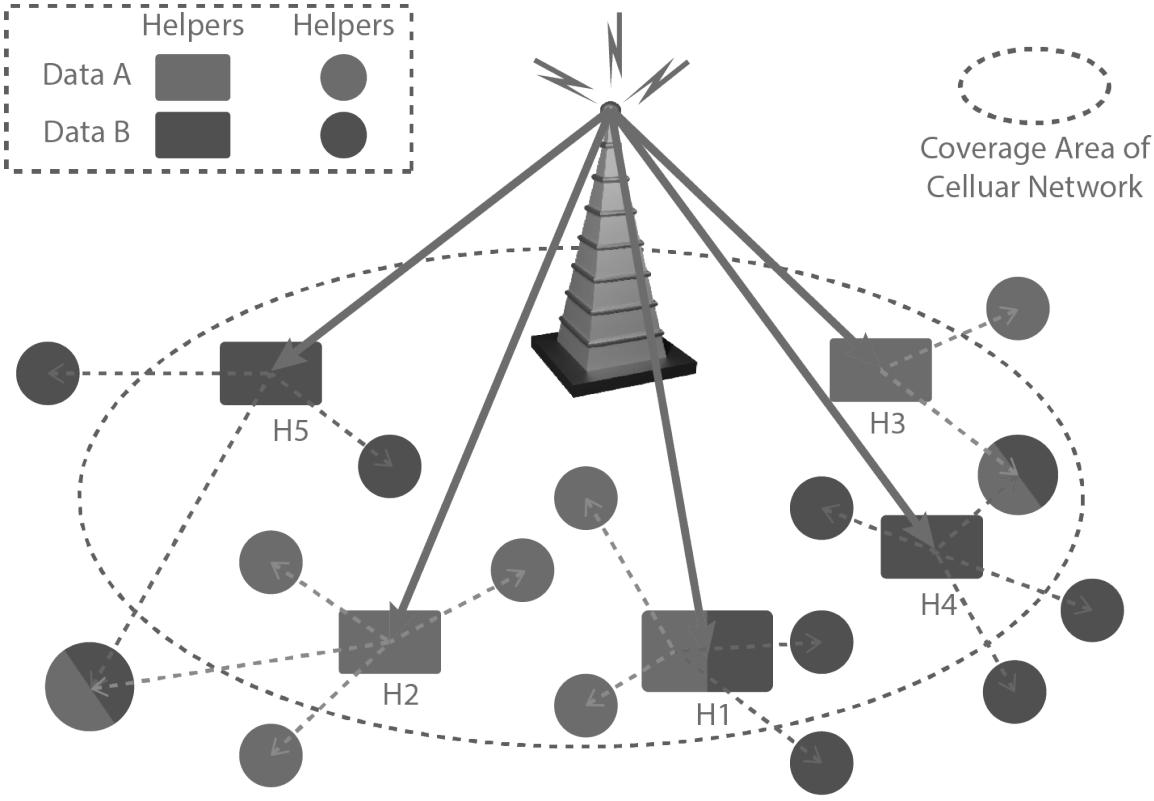
One fundamental aspect of blockchain security revolves around cryptographic protocols, such as ECC, which are instrumental in securing transactions and communications within blockchain networks. By leveraging advanced cryptographic techniques like ECC, blockchain platforms can ensure the confidentiality, integrity, and authenticity of transactions, thereby bolstering the overall security posture of the network.

Additionally, consensus mechanisms play a crucial role in blockchain security by ensuring agreement among network participants regarding the validity of transactions and the state of the ledger. Robust consensus mechanisms, such as Proof of Work (PoW) or Proof of Stake (PoS), help mitigate the risk of double-spending attacks and ensure the immutability of the blockchain.

Furthermore, network architecture considerations, such as peer-to-peer communication protocols and network topology, are essential for ensuring resilience against various types of attacks, including distributed denial-of-service (DDoS) attacks and network partitioning attacks. By designing a decentralized and fault-tolerant network architecture, blockchain platforms can enhance their resistance to malicious actors and ensure continuous operation under adverse conditions (Rithika 2022) .

Moreover, compliance with regulatory requirements and industry standards is paramount for ensuring the legality and legitimacy of blockchain-based systems. Adherence to regulations such as Know Your Customer (KYC) and Anti-Money Laundering (AML) guidelines helps mitigate the risk of illicit activities and ensures the trustworthiness of the blockchain ecosystem.

The provided Python sample code offers valuable insights into the complexities of ECC-based cryptography within blockchain networks. By understanding the intricacies involved in key generation, encryption, and decryption, NOW blockchain developers can enhance the security and privacy of transactions and communications within blockchain ecosystems. Moreover, by incorporating robust security features and adhering to best practices in NOW blockchain security, organizations can mitigate the risk of attacks and ensure the integrity and confidentiality of their blockchain-based systems (Yue 2016).



Fault Tolerant Network design for Mobile

Integrating IMEI for Enhanced Security

The International Mobile Equipment Identity (IMEI) serves as a unique identifier for mobile devices, facilitating network authentication and device tracking. Leveraging the IMEI in conjunction with ECC adds an additional layer of security to NOW Blockchain's cryptographic solutions.

By associating cryptographic keys with the IMEI of a device, NOW Blockchain can enhance the security of key management processes. This ensures that cryptographic operations are tied to specific authorized devices, mitigating the risk of unauthorized access or key compromise. Furthermore, integrating the IMEI into cryptographic protocols enables seamless integration with existing mobile infrastructure, ensuring compatibility and interoperability.

Strategic Implications for NOW Blockchain

NOW Blockchain's decision to focus on ECC within a binary field, complemented by the integration of IMEI-based security mechanisms, carries significant strategic implications. By embracing ECC, NOW Blockchain aligns itself with industry best practices and emerging cryptographic standards, enhancing its reputation as a provider of cutting-edge security solutions.

Furthermore, the emphasis on binary field implementations underscores NOW Blockchain's commitment to efficiency and scalability. By optimizing cryptographic operations for resource-constrained environments, NOW Blockchain can cater to a wide range of applications spanning mobile devices, IoT endpoints, and embedded systems.

The integration of IMEI-based security features not only enhances the robustness of NOW Blockchain's cryptographic offerings but also opens up new opportunities for collaboration with mobile network operators and device manufacturers. By leveraging existing infrastructure and standards, NOW Blockchain can position itself as a key enabler of secure mobile communications and transactions.

Enhancing NOW Blockchain Security Through Integration of Mobile Device Security Methods and Blockchain Technology

To bolster user trust and enhance security measures, the adoption of additional authentication mechanisms has gained prominence. Among these, the International Mobile Equipment Identity (IMEI) and Identity-based Public Key Cryptography (ID-based PKC) have emerged as widely utilized options. Furthermore, more sophisticated methods have been introduced, such as the management flow that integrates transaction key creation, Elliptic Curve encryption, and decryption processes to safeguard users' personal information and biometric features. Additionally, there is a growing trend towards employing multiple user-based authentication approaches, including the initialization of users' trip routes using coordinates of home and office to establish template trajectories and stay points for authentication purposes. This amalgamation of biometric-geo mobile identity authentication and various other methods underscores the multifaceted approach taken towards enhancing security and user experience (Zukarnain et al. 2022).

By delving into the intricacies of diverse security methods employed on each mobile device, such as smartphones, the NOW blockchain team has recognized an opportunity to synergize these methods to fortify the security of the NOW blockchain platform while simultaneously rewarding users for their participation and engagement. This strategic integration aims to harness the strengths of both mobile device security measures and blockchain technology to create a robust and resilient ecosystem that prioritizes user security and trust.

In building and testing its security features, NOW blockchain has undertaken a comprehensive approach that encompasses several key steps. Firstly, extensive research is conducted to understand the intricacies of existing security methods employed on mobile devices and blockchain platforms. This entails analyzing the strengths and weaknesses of various authentication mechanisms, encryption techniques, and identity verification protocols to identify areas for improvement and innovation.

Subsequently, the NOW blockchain team collaborates with experts in mobile device security, cryptography, and blockchain technology to develop novel approaches that leverage the strengths of both domains. This collaborative effort involves designing and implementing innovative security features that integrate biometric authentication, cryptographic protocols, and blockchain technology to enhance the overall security posture of the NOW blockchain platform.

Moreover, rigorous testing and validation processes are continuing and being conducted to assess the effectiveness and robustness of the implemented security features before the launch of main net. This entails conducting comprehensive security audits, penetration testing, and simulation exercises to identify and mitigate potential vulnerabilities and security risks. Additionally, user feedback and engagement are solicited to ensure that the implemented security measures are user-friendly, intuitive, and aligned with user expectations.

Utilization of Ethereum Virtual Machine (EVM) in NOW Blockchain

The Ethereum Virtual Machine (EVM) serves as a pivotal component within the blockchain ecosystem, facilitating the execution of smart contracts and decentralized applications (dApps) on the Ethereum network. Since its inception, the EVM has garnered widespread recognition for its robustness and versatility, leading several blockchain networks to adopt its architecture to

harness its capabilities. NOW Blockchain emerges as one of the select few blockchains, alongside Binance Smart Chain, Polygon, Avalanche, Fantom, Solana, and Tron, that leverage the EVM for smart contract execution and dApp development. This section delves into the significance of NOW Blockchain's utilization of the EVM within the broader context of blockchain interoperability and innovation.

Importance of EVM Utilization

The decision to integrate the Ethereum Virtual Machine (EVM) into NOW Blockchain underscores the platform's commitment to interoperability and compatibility with the broader Ethereum ecosystem. By adopting the EVM, NOW Blockchain inherits compatibility with a vast array of Ethereum-based smart contracts and dApps, thereby expanding its utility and appeal to developers and users alike. This interoperability facilitates seamless asset transfers and data exchange between NOW Blockchain and other EVM-compatible networks, fostering a more interconnected and vibrant blockchain ecosystem.

Enhanced Interoperability and Collaboration

NOW Blockchain's utilization of the Ethereum Virtual Machine (EVM) not only enables compatibility with Ethereum-based applications but also promotes cross-chain interoperability with other EVM-utilizing blockchains. This interoperability enhances the platform's versatility and opens up new avenues for collaboration and innovation within the cryptocurrency space. Developers can leverage NOW Blockchain's EVM compatibility to deploy decentralized applications that seamlessly interact with assets and protocols across multiple blockchain networks, thereby tapping into a broader user base and liquidity pool.

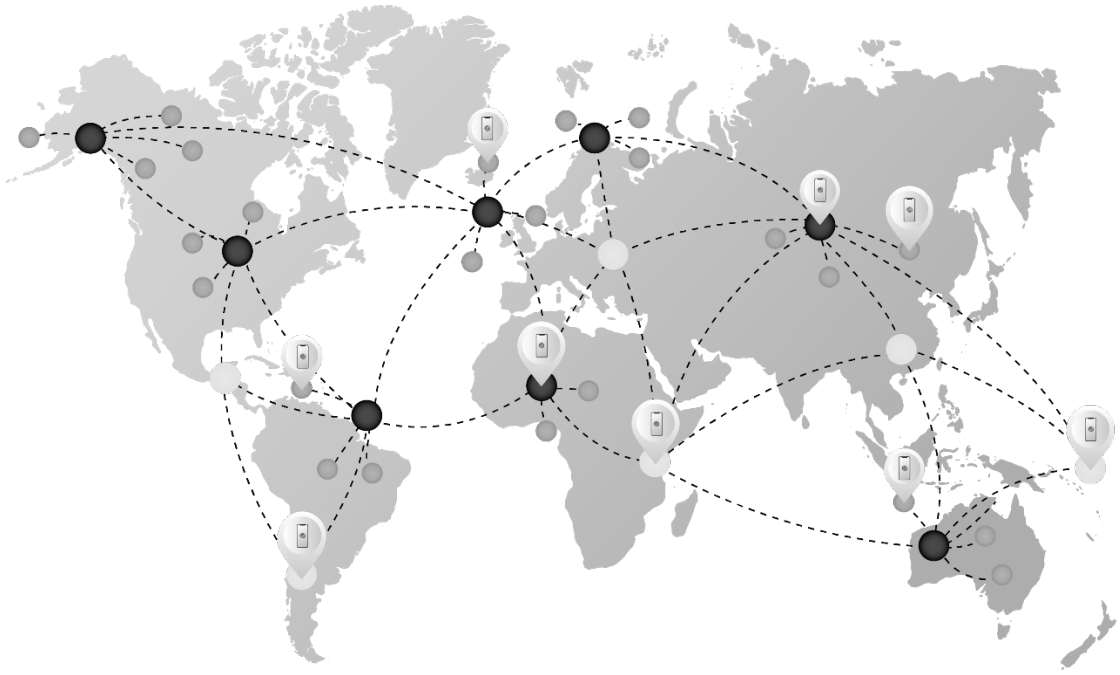
Supporting Evidence

According to Ethereum's official documentation on the Ethereum Virtual Machine (EVM) as accessed on November 7, 2023, the EVM serves as the runtime environment for executing smart contracts on the Ethereum blockchain (Ethereum Foundation, 2023). This documentation elucidates the fundamental role of the EVM in facilitating smart contract execution and highlights its significance within the Ethereum ecosystem.

NOW Blockchain's adoption of the Ethereum Virtual Machine (EVM) underscores its commitment to interoperability, innovation, and compatibility with the broader Ethereum ecosystem. By leveraging the EVM, NOW Blockchain aligns itself with prominent blockchain networks such as Binance Smart Chain, Polygon, Avalanche, Fantom, Solana, and Tron, that utilize the same architecture, thereby enhancing its appeal to developers and users seeking a familiar and versatile platform for deploying decentralized applications. The utilization of the EVM positions NOW Blockchain as a key player in the evolving landscape of blockchain technology, poised to contribute to the proliferation of decentralized finance (DeFi) and decentralized applications (dApps) in the years to come.

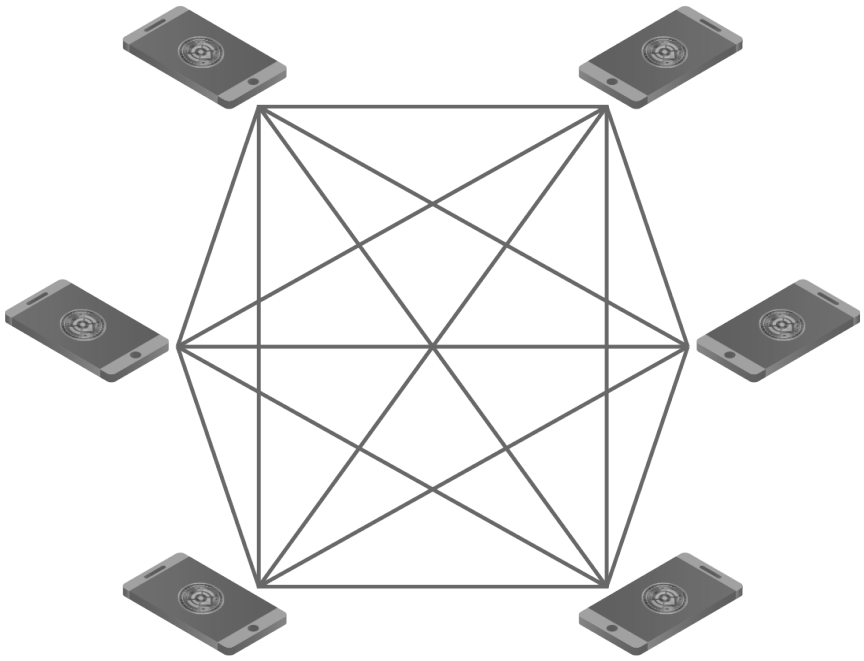
Proof of Mobile (PoM): A Consensus Mechanism for the Mobile Era

As the world becomes increasingly reliant on mobile devices for communication, commerce, and social interaction, the need for efficient and secure consensus mechanisms tailored to the unique challenges of the mobile environment becomes more apparent. Traditional consensus mechanisms, such as Proof of Work (PoW) and Proof of Stake (PoS), have been the cornerstone of blockchain networks, ensuring agreement on the state of the ledger in a decentralized manner. However, the resource-intensive nature of PoW and the potential centralization risks associated with PoS present obstacles in the mobile context. In response to these challenges, Proof of Mobility (PoM) emerges as a promising alternative, offering a novel approach to achieving consensus in mobile-centric networks. PoM leverages the inherent mobility of devices and their ability to verify transactions and participate in the consensus process. This essay aims to provide a comprehensive exploration of PoM, elucidating its underlying principles, mechanisms, advantages, and potential applications in the mobile era.



At its core, PoM is a consensus mechanism that validates and secures transactions by leveraging the mobility patterns of users' devices. Unlike PoW, which requires miners to solve complex cryptographic puzzles to validate transactions, or PoS, which relies on participants staking their cryptocurrency holdings to verify transactions, PoM introduces a paradigm shift by utilizing the physical movement of mobile devices as a means of reaching consensus. This innovative approach not only addresses the limitations of traditional consensus mechanisms in the mobile context but also opens up new opportunities for building decentralized networks that are efficient, secure, and inclusive.

The concept of PoM revolves around the notion that the movement of mobile devices can serve as a proxy for computational work or stake in traditional consensus mechanisms. By harnessing the GPS or location data of mobile devices, PoM algorithms can ascertain the physical proximity of devices to one another, establishing trust and enabling them to collectively validate transactions. This reliance on mobility introduces a dynamic element into the consensus process, as the validation power of a device is directly proportional to its mobility and network participation. In essence, the more actively a device moves and interacts within the network, the greater its influence on the consensus outcome, thus incentivizing users to actively engage with the network and contribute to its security and integrity.



One of the key advantages of PoM is its ability to mitigate the centralization risks inherent in PoW and PoS. In traditional PoW systems, the concentration of mining power among a few entities or mining pools can lead to a centralized control of the network, jeopardizing its decentralization and security. Similarly, PoS mechanisms may suffer from centralization tendencies, as participants with a large stake in the network wield disproportionate influence over the consensus process. In contrast, PoM distributes validation authority based on the decentralized movement of mobile devices, reducing the risk of centralization and fostering a more democratic and inclusive network architecture. Since mobility is inherently distributed and decentralized, PoM aligns with the principles of decentralization, ensuring that no single entity can dominate the consensus process or manipulate the network for its gain.

Furthermore, PoM offers significant energy efficiency benefits compared to PoW, which requires vast computational resources and energy consumption to validate transactions. The mining process in PoW-based cryptocurrencies like Bitcoin consumes enormous amounts of electricity, raising concerns about its environmental impact and sustainability. In contrast, PoM harnesses

the natural movement of mobile devices, which incurs minimal additional energy consumption beyond the device's regular operation. This eco-friendly approach not only reduces the carbon footprint associated with consensus mechanisms but also makes blockchain technology more accessible to regions with limited energy infrastructure, where mobile devices are prevalent but electricity is scarce.

In addition to its energy efficiency, PoM enhances the scalability and throughput of blockchain networks, making them better suited for real-time transactions and applications. The dynamic nature of mobile devices enables PoM-based networks to adapt to varying transaction volumes and network conditions, ensuring high throughput and low latency even during peak usage periods. This scalability is particularly crucial for mobile-centric applications, such as mobile payments, IoT (Internet of Things) devices, and location-based services, where speed and responsiveness are paramount. By leveraging the collective mobility of devices, PoM can process transactions more efficiently and reliably, laying the groundwork for a new generation of decentralized applications optimized for mobile environments.

Moreover, PoM introduces innovative incentive mechanisms to encourage active participation and engagement within the network. In traditional consensus mechanisms, participants are typically rewarded with newly minted coins or transaction fees for their contribution to the network's security and validation process. While these incentives remain relevant in PoM-based networks, additional rewards can be offered based on the mobility and interaction patterns of devices. For example, devices that actively participate in transaction validation or contribute to network propagation by relaying data may earn bonus rewards or reputation points. This gamified approach not only incentivizes users to actively engage with the network but also fosters a sense of community and collaboration among participants.

In conclusion, Proof of Mobility (PoM) represents a groundbreaking approach to achieving consensus in mobile-centric blockchain networks. By leveraging the inherent mobility of devices, PoM introduces a dynamic and decentralized consensus mechanism that addresses the limitations of traditional PoW and PoS mechanisms in the mobile context. With its energy efficiency, scalability, and innovative incentive structures, PoM has the potential to revolutionize the way we think about consensus in the mobile era, opening up new possibilities for decentralized applications and services optimized for mobile environments. As the adoption of mobile devices continues to grow worldwide, PoM stands poised to play a pivotal role in shaping the future of blockchain technology and decentralized systems.

Legal Disclaimer:

Nothing in this White Paper constitutes an offer to sell, or solicitation of an offer to purchase, any tokens associated with NOW blockchain. NOW blockchain is presenting this White Paper solely for the purpose of gathering feedback and comments from the public. Any future offering of tokens by NOW blockchain, including through a Simple Agreement for Future Tokens (SAFT), will be conducted through definitive offering documents, which will include a disclosure document and risk factors. These definitive documents may contain an updated version of this White Paper, which could differ significantly from the current version. In the event of an offering in the United States, it is anticipated that the offering will be limited to accredited investors.

It is important to note that nothing in this White Paper should be construed as a guarantee or promise regarding the development of NOW blockchain or the tokens it offers, nor as an assurance of the utility or value of the tokens. The contents of this White Paper outline current plans, which are subject to change at the discretion of NOW blockchain, and their success will depend on numerous factors beyond NOW blockchain's control, including market conditions and developments within the data and cryptocurrency industries. Any statements regarding future events are based solely on NOW blockchain's analysis of the issues discussed in this White Paper, which may ultimately prove to be inaccurate.

Furthermore, it should be acknowledged that the Proof of Mobile (PoM) consensus mechanism mentioned within this White Paper is currently a work in progress. While NOW blockchain is actively researching and developing this consensus model, its implementation and effectiveness have not yet been fully realized. As such, the inclusion of PoM in this White Paper does not imply its immediate availability or functionality within the NOW blockchain ecosystem. Any updates or developments regarding the PoM consensus mechanism will be communicated through official channels as the project progresses.

References:

Marr, B. (2023, April 14). The 5 Biggest Problems with Blockchain Technology Everyone Must Know About. *Forbes*. https://www.forbes.com/sites/bernardmarr/2023/04/14/the-5-biggest-problems-with-blockchain-technology-everyone-must-know-about/?sh=2b60dcc355d2

Statista. (n.d.). Global smartphone users forecast. Retrieved from https://www.statista.com/forecasts/1143723/smartphone-users-in-the-world#statisticContainer

Iredale, G. (2021, April 23). Blockchain Cryptography: Everything You Need to Know. Retrieved from https://101blockchains.com/blockchain-cryptography/?sscid=31k8_jke21

Bhat, J. (2021, August). Image Encryption Using Logistic-Cosine-Sine Chaos Map and Elliptic Curve Cryptography. ResearchGate. https://www.researchgate.net/publication/354808660_IMAGE_ENCRYPTION_USING_LOGISTIC-COSINE-SINE_CHAOS_MAP_AND_ELLIPTIC_CURVE_CRYPTOGRAPHY

Seth, S. (2022, May 15). Explaining Cryptography in Blockchain. Investopedia. https://www.investopedia.com/tech/explaining-crypto-cryptocurrency/#:~:text=The%20second%20method%20is%20Asymmetric%20Encryption,is%20known%20only%20to%20the%20owner.&text=The%20second%20method%20is,only%20to%20the%20owner.&text=method%20is%20Asymmetric%20Encryption,is%20known%20only%20to.

IBM. (n.d.). Blockchain Security. Retrieved from https://www.ibm.com/topics/blockchain-security

Shamsher Ullah, Jiangbin Zheng, Nizamud Din, Muhammad Tanveer Hussain, Farhan Ullah, Mahwish Yousaf. (February 2023). Advancements in Asymmetric Encryption: A Comprehensive Analysis. Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S1574013722000648

Arampatzis, A. (June 16, 2023). What Asymmetric Encryption Is and When to Use It. Retrieved from https://venafi.com/blog/what-asymmetric-encryption-is-and-when-to-use-it/

Kumar Sharma, T. (June 23, 2018). How Does Blockchain Use Public Key Cryptography? Retrieved from https://www.blockchain-council.org/blockchain/how-does-blockchain-use-public-key-cryptography/

Poggi, N. (June 15, 2021). Types of Encryption: Symmetric or Asymmetric, RSA or AES? Retrieved from https://preyproject.com/blog/types-of-encryption-symmetric-or-asymmetric-rsa-or-aes

Abdurahmonov, T., Yeoh, E. T., & Hussain, H. M. (2011). Improving smart card security using elliptic curve cryptography over prime field (fp). In Software engineering, artificial intelligence, networking and parallel/distributed computing (pp. 127–140). Springer.

Anoop, M. S. (2007). Elliptic curve cryptography, an implementation guide. Online Implementation Tutorial, Tata Elxsi, India.

Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., & Rajarajan, M. (2013). A survey of intrusion detection techniques in cloud. Journal of Network and Computer Applications, 36(1), 42–57.

Dhor, Partho Sutra. (2022). The Mathematics Behind Blockchain. IEEE TechBriefs, 2022(Q3). Retrieved from https://blockchain.ieee.org/images/files/pdf/techbriefs-2022-q3/the-mathematics-behind-blockchain.pdf

Nakov, Seflin. (2018, November). Elliptic Curve Cryptography (ECC). CryptoBook. Retrieved from https://cryptobook.nakov.com/asymmetric-key-ciphers/elliptic-curve-cryptography-ecc

Munir, M. Y. (January 1, 2023). Blockchain Security: Understanding and Preventing Common Attacks. Retrieved from https://www.linkedin.com/pulse/blockchain-security-understanding-preventing-common-attacks-munir#:~:text=Some%20of%20the%20most%20common%20attacks%20on%20blockchain,man-in-the-middle%20attacks%2C%20DDoS%20attacks%2C%20and%20smart%20contract%20vulnerabilities.

GeeksforGeeks. (n.d.). Blockchain - Elliptic Curve Cryptography. Retrieved from https://www.geeksforgeeks.org/blockchain-elliptic-curve-cryptography/

Rithika, Sharon (May 9, 2022) The Ultimate Guide On Designing a Fault Tolerant Network 101. Retrieved from https://hevodata.com/learn/fault-tolerant-network/

Yue, Frank (February 9, 2016). An Introductory Guide to Developing Fault-Tolerant Networks. Retrieved from https://www.radware.com/blog/applicationdelivery/2016/02/an-introductory-guide-to-developing-fault-tolerant-networks/

Liljeqvist, I. (October 7, 2022). What Are Consensus Mechanisms? Retrieved from https://academy.moralis.io/blog/what-are-consensus-mechanisms

Mansa, J. (February 17, 2023). Consensus Mechanism. Investopedia. Retrieved from https://www.investopedia.com/terms/c/consensus-mechanism-cryptocurrency.asp

Zukarnain, Z. A., Muneer, A., & Aziz, M. K. A. (2022, March 13). Combining Mobile Device Security Methods and Blockchain to Improve NOW Blockchain Security. Retrieved from https://www.mdpi.com/2073-8994/14/4/821.

Ethereum Foundation. (2023, November 7). Ethereum Virtual Machine (EVM). Retrieved from https://ethereum.org/en/developers/docs/evm/

A Chain is No Stronger Than its Weakest Link

William James