NCRYPT

A Quantum-Resistant Blockchain Platform

Whitepaper v1.0

Secure. Private. Accountable. Future-Proof.

Table of Contents

1. Executive Summary

NCRYPT represents a paradigm shift in blockchain technology, designed from the ground up to address the existential threat posed by quantum computing to current cryptographic systems. As quantum computers advance toward breaking classical cryptography, traditional blockchains face a critical vulnerability that could compromise billions of dollars in digital assets.

NCRYPT is a next-generation, quantum-resistant Layer 1 blockchain platform that combines post-quantum cryptography with a flexible, multi-tier privacy architecture. Unlike existing solutions that offer binary privacy choices, NCRYPT enables users to select between transparent, fully private, or accountable transaction modes, addressing both individual privacy needs and institutional compliance requirements.

Built upon lattice-based cryptographic primitives recommended by NIST for post-quantum security, NCRYPT employs Module-LWE (Learning With Errors) and Module-SIS (Short Integer Solution) schemes that have been extensively vetted by the cryptographic community. These primitives provide quantum resistance without requiring hard forks or disruptive upgrades.

The platform introduces the DAPOA (Decentralized Anonymous Payment with Optional Accountability) framework, which enables mathematically provable privacy guarantees while allowing selective disclosure to authorized auditors. This unique capability positions NCRYPT as the first quantum-resistant blockchain that can simultaneously preserve user anonymity and meet regulatory requirements such as AML/KYC compliance.

NCRYPT aims to become the foundational infrastructure for secure, private, and compliant digital value exchange in the quantum era. By combining cutting-edge cryptography with practical regulatory considerations, NCRYPT bridges the gap between maximalist privacy coins and fully transparent blockchains, offering a balanced solution for individuals, enterprises, and institutions alike.

2. Introduction

2.1 The Evolution of Blockchain Security

Since Bitcoin's introduction in 2009, blockchain technology has revolutionized how we think about digital value, trust, and decentralized systems. However, the cryptographic foundations upon which these systems are built—primarily elliptic curve cryptography (ECC) and RSA—were designed decades before quantum computing became a tangible threat.

The blockchain ecosystem has evolved to address various challenges: scalability, privacy, and regulatory compliance. Projects like Monero and Zcash pioneered privacy-preserving transactions, while platforms like Ethereum introduced programmability. Yet, none of these solutions adequately address the quantum threat that looms on the horizon.

2.2 The Privacy-Compliance Dilemma

A fundamental tension exists in the cryptocurrency space between privacy advocates who demand complete anonymity and regulatory authorities who require transparency for compliance. This dichotomy has forced institutions to choose between fully transparent blockchains that compromise user privacy or privacy coins that face regulatory scrutiny.

NCRYPT solves this dilemma by introducing selectable privacy levels, allowing users to choose their preferred balance between privacy and accountability based on their specific needs and regulatory obligations.

2.3 The NCRYPT Solution

NCRYPT addresses three critical challenges facing the blockchain ecosystem:

- Quantum Vulnerability: Classical cryptographic systems will be broken by sufficiently powerful quantum computers, threatening all existing blockchain security.
- Privacy Limitations: Most blockchains offer binary choices—either fully transparent or fully private—with no middle ground for institutions requiring selective accountability.
- Regulatory Compliance: Privacy coins face increasing regulatory pressure, while transparent blockchains sacrifice user privacy for compliance.

NCRYPT provides a comprehensive solution that addresses all three challenges simultaneously, creating a blockchain platform that is secure against quantum threats, privacy-preserving, and regulatory-compliant.

3. The Quantum Threat

3.1 Understanding Quantum Computing

Quantum computing leverages quantum mechanical phenomena—superposition and entanglement—to perform computations that would be infeasible for classical computers. While quantum computers excel at specific problems like factoring large integers and solving discrete logarithm problems, they represent an existential threat to current cryptographic systems.

The two primary quantum algorithms threatening classical cryptography are:

- Shor's Algorithm: Can factor large integers and compute discrete logarithms in polynomial time, breaking RSA and ECC-based systems.
- Grover's Algorithm: Provides a quadratic speedup for unstructured search problems, effectively halving the security of symmetric cryptographic algorithms.

3.2 Timeline to Quantum Supremacy

While estimates vary, the cryptographic community generally expects that large-scale quantum computers capable of breaking current cryptography will emerge within the next 10-30 years. However, the threat exists today through "harvest now, decrypt later" attacks, where adversaries collect encrypted data with the intention of decrypting it once quantum computers become available.

The National Institute of Standards and Technology (NIST) has been leading an initiative to standardize post-quantum cryptographic algorithms, recognizing the urgency of transitioning to quantum-resistant cryptography before the threat materializes.

3.3 Impact on Existing Blockchains

Virtually all major blockchain platforms rely on cryptographic assumptions that will be broken by quantum computers:

- Bitcoin and Ethereum: Use ECDSA (Elliptic Curve Digital Signature Algorithm) for transaction signing, which is vulnerable to Shor's algorithm.
- Privacy Coins: Monero and Zcash use quantum-vulnerable cryptographic primitives in their privacy mechanisms.
- Smart Contracts: Many DeFi protocols rely on quantum-vulnerable signatures and hash functions.

A successful quantum attack on any major blockchain could result in the theft of billions of dollars in digital assets, potentially destroying trust in the entire ecosystem. The transition to post-quantum cryptography is not optional—it is essential for the long-term viability of blockchain technology.

4. Vision and Objectives

4.1 Core Vision

NCRYPT envisions a future where blockchain technology provides robust security against both classical and quantum threats while offering flexible privacy options that accommodate diverse user needs—from privacy-maximizing individuals to compliance-requiring institutions.

4.2 Primary Objectives

4.2.1 Quantum Resistance

NCRYPT employs lattice-based cryptographic primitives (Module-LWE and Module-SIS) that have been extensively studied by the cryptographic community and recommended by NIST for post-quantum security. These primitives are believed to be secure against both classical and quantum computers.

Unlike systems that require hard forks to upgrade cryptography, NCRYPT is quantum-resistant by design from day one, ensuring long-term security without disruptive upgrades.

4.2.2 Multi-Tier Privacy

NCRYPT provides three distinct privacy levels, allowing users to select the appropriate balance between privacy and accountability:

Basic Privacy (Transparent Mode):
Similar to Bitcoin, transactions are publicly visible on the blockchain. Quantum-resistant one-time wallet addresses provide basic privacy by preventing address reuse. This mode is suitable for public audits, transparency requirements, and use cases where privacy is not a primary concern.**Full Privacy (Private Mode):**
Addresses, transaction amounts, and sender-receiver relationships are all concealed using zero-knowledge proofs and homomorphic commitments. This mode provides maximum privacy, similar to Monero or Zcash, but with quantum-resistant cryptography.**Full Privacy with Accountability (Accountable Mode):**
Transactions are private to all parties except authorized auditors or regulators who possess tracking keys. This mode enables selective disclosure of transaction details for compliance purposes while maintaining privacy from unauthorized parties. This unique capability allows institutions to meet AML/KYC requirements without sacrificing user anonymity.

4.2.3 Regulatory Compliance

Through the accountable privacy mode, NCRYPT enables institutions to meet regulatory requirements including:

- Anti-Money Laundering (AML) compliance through selective transaction tracing
- Know Your Customer (KYC) requirements via controlled identity disclosure
- Tax reporting through verifiable transaction proofs
- Audit trails for regulated financial services

This capability positions NCRYPT as the first quantum-resistant blockchain that can serve institutional use cases requiring both privacy and compliance.

4.2.4 Provable Security

NCRYPT provides mathematically provable security guarantees for privacy, anonymity, and accountability. All cryptographic primitives are based on well-studied hardness assumptions with formal security proofs, ensuring users can trust in the system's security properties.

5. Technical Architecture

5.1 Cryptographic Foundations

NCRYPT's security rests on lattice-based cryptography, specifically Module-LWE and Module-SIS problems, which are believed to be hard for both classical and quantum computers. These primitives form the foundation for all security-critical operations in the system.

5.1.1 Module-LWE (Learning With Errors)

Module-LWE provides the hardness assumption for public-key encryption and digital signatures. The problem involves distinguishing between noisy inner products and truly random values in a module over a polynomial ring, which remains hard even for quantum algorithms.

5.1.2 Module-SIS (Short Integer Solution)

Module-SIS provides the hardness assumption for hash functions and commitment schemes. The problem requires finding short vectors in a module lattice, which is believed to be computationally infeasible for both classical and quantum computers.

5.1.3 Post-Quantum Primitives

NCRYPT employs the following cryptographic building blocks, all quantum-resistant:

- Lattice-based digital signatures (Module-LWE/SIS-based schemes like Dilithium or Falcon)
- Homomorphic commitments for encrypted transaction amounts
- Zero-knowledge range proofs for value validation
- Linkable ring signatures for unlinkability in private transactions
- Verifiable encryption for controlled accountability

5.2 Data Model

NCRYPT uses a UTXO (Unspent Transaction Output) model similar to Bitcoin, but with enhanced privacy capabilities. Three types of transaction outputs are supported:

Public TXOs:
Fully transparent outputs where addresses and amounts are visible on the blockchain. Suitable for transparent mode transactions.

Value-Hidden TXOs:
Amounts are encrypted using homomorphic commitments, while addresses remain visible. Provides partial privacy for accountable mode transactions.

Private TXOs:
Both addresses and amounts are concealed using zero-knowledge proofs and ring signatures. Provides maximum privacy for private mode transactions.

5.3 Transaction Types

NCRYPT supports four primary transaction types that enable conversion between privacy modes:

- Public Transaction: Creates public TXOs. Fully transparent blockchain activity suitable for public audits.

• Mask Transaction: Converts public outputs to value-hidden outputs, enabling partial privacy with accountability.

• Private Transaction: Creates private TXOs with concealed addresses and amounts, providing maximum privacy.

• Unmask Transaction: Converts private or value-hidden outputs back to public outputs, enabling selective transparency.

This flexible transaction model allows users to adapt their privacy level based on changing requirements without being locked into a single mode.

5.4 Account Model

While NCRYPT uses a UTXO model for transaction processing, users interact with the system through accounts that abstract away UTXO management. Accounts can generate one-time addresses for each transaction, providing basic privacy even in transparent mode.

6. Privacy Framework

6.1 Privacy Levels

NCRYPT's multi-tier privacy framework enables users to select privacy levels that match their specific needs:

6.1.1 Transparent Mode

In transparent mode, all transaction data is publicly visible on the blockchain, similar to Bitcoin. However, NCRYPT enhances basic privacy through:

- One-time wallet addresses prevent address reuse and basic transaction graph analysis
- Quantum-resistant address generation ensures long-term security
- Optional account abstraction for user-friendly interfaces

Use cases include public audits, transparency requirements, and scenarios where privacy is not a concern.

6.1.2 Private Mode

Private mode provides maximum anonymity through multiple privacy-enhancing techniques:

- Ring signatures hide the actual sender among a group of potential senders
- Stealth addresses conceal recipient addresses from observers
- Homomorphic commitments encrypt transaction amounts
- Zero-knowledge range proofs ensure amounts are valid without revealing their values

Transactions in private mode are unlinkable and untraceable by anyone except authorized auditors with tracking keys.

6.1.3 Accountable Mode

Accountable mode provides the unique capability of selective disclosure:

- Transactions appear private to regular users and observers
- Authorized auditors with tracking keys can selectively reveal transaction details
- Compliance proofs enable institutions to demonstrate regulatory adherence
- User anonymity is preserved from all unauthorized parties

This mode enables institutions to meet AML/KYC requirements while maintaining user privacy, solving the privacy-compliance dilemma.

6.2 Privacy Guarantees

NCRYPT provides formal privacy guarantees through cryptographic proofs:

- Anonymity: Sender and receiver identities are unlinkable from transactions
- Unlinkability: Multiple transactions cannot be linked to the same user
- Untraceability: Transaction histories cannot be traced through the blockchain
- Confidentiality: Transaction amounts are concealed in private/accountable modes

6.3 Privacy vs. Compliance Trade-offs

Different privacy levels offer different trade-offs:

- Transparent mode: Maximum compliance, minimum privacy
- Private mode: Maximum privacy, no compliance capabilities
- Accountable mode: Balanced privacy and compliance through selective disclosure

Users can switch between modes based on their evolving needs, providing unprecedented flexibility in privacy management.

7. DAPOA Model

7.1 Overview

DAPOA (Decentralized Anonymous Payment with Optional Accountability) is NCRYPT's core privacy framework, enabling mathematically provable privacy guarantees while supporting selective disclosure for compliance.

7.2 Core Properties

DAPOA ensures four fundamental properties:

7.2.1 Anonymity

Sender and receiver identities are cryptographically hidden. Even in accountable mode, transactions appear anonymous to all parties except authorized auditors.

7.2.2 Value Hiding

Transaction amounts are encrypted using homomorphic commitments, allowing verification of transaction validity without revealing amounts.

7.2.3 Consumed Coin Hiding

Input-output relationships are concealed using ring signatures, preventing transaction graph analysis.

7.2.4 Optional Accountability

Transactions may embed tracking public keys that enable authorized parties (regulators, auditors) to selectively reveal transaction details for compliance purposes.

7.3 Tracking Keys

In accountable mode, transactions can include a tracking public key generated by an authorized auditor or regulator. This key enables:

- Selective transaction tracing for AML compliance
- Controlled identity disclosure for KYC requirements
- Audit trail generation without compromising general user privacy
- Regulatory reporting while maintaining user anonymity from unauthorized parties

Users can opt into accountable mode when transacting with regulated entities, providing the transparency needed for compliance without sacrificing privacy elsewhere.

7.4 Security Properties

DAPOA provides formal security guarantees:

- Computational anonymity: Breaking anonymity requires solving hard cryptographic problems
- Zero-knowledge privacy: Privacy does not depend on trusted parties or security assumptions
- Selective disclosure: Only authorized parties with tracking keys can reveal transaction details
- Non-repudiation: Audit proofs are cryptographically verifiable and cannot be forged

8. Consensus Mechanism

8.1 Initial Proof-of-Work Phase

NCRYPT will launch with a Proof-of-Work (PoW) consensus mechanism to ensure:

- Maximum decentralization during the initial distribution phase
- Sybil resistance without requiring trusted setups
- Fair token distribution through mining
- Security through computational work

The PoW algorithm uses a quantum-resistant hash function to ensure miners cannot leverage quantum advantages, maintaining fairness and security.

8.2 Transition to Proof-of-Stake

After the initial distribution phase, NCRYPT will transition to a Proof-of-Stake (PoS) consensus mechanism to:

- Reduce energy consumption by orders of magnitude
- Improve transaction throughput and finality times
- Enable more efficient network participation
- Support long-term sustainability

The transition will be carefully planned and executed through community governance, ensuring network security throughout the process.

8.3 Stake-Based Security

The PoS mechanism will feature:

- Economic security through stake-weighted consensus
- Slashing penalties for malicious behavior
- Delegated staking for accessibility
- Quantum-resistant signature schemes for validator operations

8.4 Network Parameters

Key network parameters include:

- Block time: ~60 seconds for fast confirmation
- Block size: Optimized for privacy-preserving transactions
- Finality: Multiple confirmation blocks for security
- Scalability: Designed to support high transaction throughput

9. Tokenomics

9.1 Token Supply

NCRYPT will have a capped supply of 21 million NCR tokens, similar to Bitcoin's supply model. This fixed supply ensures:

- Predictable monetary policy without inflation
- Scarcity value similar to digital gold
- Long-term value preservation
- Protection against currency debasement

9.2 Token Distribution

The initial token distribution is designed to balance fairness, network security, and long-term development:

Mining/Staking Rewards (60%):
The majority of tokens are distributed through mining (PoW phase) and staking (PoS phase), ensuring decentralized distribution and network security.

Ecosystem Development (20%):
Reserved for grants, partnerships, and ecosystem incentives to accelerate adoption and development.

Partnerships & R&D (10%):
Allocated for strategic partnerships, research initiatives, and technological advancement.

Team & Early Contributors (10%):
Vested over multiple years to align team incentives with long-term project success.

9.3 Token Utility

NCR tokens serve multiple purposes in the NCRYPT ecosystem:

- Transaction Fees: Required for all blockchain transactions
- Staking: Locking tokens for network security and consensus participation
- Governance: Voting rights for protocol upgrades and parameter changes
- Ecosystem Access: Required for advanced features and premium services
- Liquidity: Trading pairs on decentralized and centralized exchanges

9.4 Monetary Policy

NCRYPT employs a deflationary monetary policy where:

- No new tokens are created after the cap is reached
- Transaction fees may be burned to reduce supply over time
- Token scarcity increases with adoption

This model ensures long-term value preservation and aligns with principles of sound money.

10. Governance

10.1 On-Chain Governance

NCRYPT will implement an on-chain governance system where token holders can propose and vote on protocol changes. This ensures decentralized decision-making and community-driven development.

10.2 Governance Proposals

The governance system enables proposals for:

- Protocol upgrades and parameter changes
- Consensus mechanism transitions
- Ecosystem fund allocations
- Technical improvements and optimizations

10.3 Voting Mechanism

Voting will be conducted through:

- Stake-weighted voting to ensure alignment with network security
- Time-locked proposals for community review
- Quorum requirements to ensure meaningful participation
- Transparent vote tracking on-chain

10.4 Governance Evolution

The governance system will evolve based on community needs, potentially incorporating:

- Delegation mechanisms for efficient participation
- Reputation systems for proposal evaluation
- Multi-sig governance for critical decisions
- Constitutional rules to protect core protocol properties

11. Security Analysis

11.1 Cryptographic Security

NCRYPT's security rests on well-studied cryptographic assumptions:

- Module-LWE and Module-SIS hardness assumptions, believed secure against quantum computers
- Formal security proofs for privacy and accountability properties
- NIST-standardized algorithms wherever possible
- Continuous security audits by independent researchers

11.2 Network Security

Network-level security is ensured through:

- Consensus mechanism providing Byzantine fault tolerance
- Economic security through staking penalties
- Peer-to-peer network design preventing single points of failure
- Regular security updates and patches

11.3 Privacy Security

Privacy guarantees are maintained through:

- Cryptographic proofs that privacy cannot be broken without solving hard problems
- Zero-knowledge proofs ensuring no information leakage
- Formal verification of privacy properties where possible
- Regular privacy audits and reviews

11.4 Attack Vectors and Mitigations

NCRYPT addresses potential attack vectors:

- Quantum attacks: Mitigated through post-quantum cryptography
- 51% attacks: Mitigated through consensus security and economic penalties
- Privacy leaks: Mitigated through cryptographic proofs and careful implementation
- Regulatory pressure: Mitigated through accountable mode enabling compliance

Ongoing security research and audits ensure continuous improvement of security measures.

12. Roadmap

12.1 Phase 1: Foundation (Q1-Q2 2026)

Objectives:

- Complete technical whitepaper and detailed architecture specifications
- Implement core cryptographic primitives and test in isolation
- Develop proof-of-concept implementation
- Conduct initial security audits
- Build development community and partnerships

12.2 Phase 2: Testnet Launch (Q3 2026)

Deliverables:

- Public testnet with core functionality
- Quantum-safe wallet applications
- Private transaction capabilities
- Developer documentation and tooling
- Community feedback integration

12.3 Phase 3: Mainnet Beta (Q1 2027)

Features:

- Mainnet launch with full quantum resistance
- All three privacy modes operational
- DAPOA privacy framework fully implemented
- Basic governance system
- Exchange listings and liquidity

12.4 Phase 4: Governance Launch (Q3 2027)

Enhancements:

- Transition to Proof-of-Stake consensus
- Full on-chain governance
- Advanced features and optimizations
- Institutional integration tools

12.5 Phase 5: Expansion (2028+)

Future developments:

- Sidechain support for scalability
- Smart contract capabilities
- Web3 integration and DeFi protocols
- Enterprise solutions and partnerships
- Cross-chain interoperability

13. Competitive Analysis

13.1 Comparison with Existing Blockchains

NCRYPT differentiates itself from existing solutions through unique capabilities:

Bitcoin:
Quantum-vulnerable ECDSA signatures; fully transparent; no privacy features. NCRYPT offers quantum resistance and selectable privacy.

Ethereum:
Quantum-vulnerable cryptography; transparent by default; smart contracts available. NCRYPT focuses on quantum resistance and privacy-first design.

Monero:
Quantum-vulnerable ring signatures; maximum privacy; no compliance capabilities. NCRYPT adds quantum resistance and accountable mode.

Zcash:
Quantum-vulnerable zk-SNARKs; optional privacy; limited compliance. NCRYPT provides quantum resistance and institutional compliance features.

13.2 Competitive Advantages

NCRYPT's unique value proposition includes:

- Only quantum-resistant blockchain with selectable privacy levels
- First privacy coin that enables regulatory compliance without sacrificing anonymity
- Future-proof security against quantum threats
- Flexible privacy framework accommodating diverse user needs
- Institutional-grade compliance capabilities

14. Use Cases

14.1 Individual Users

Privacy-conscious individuals can use NCRYPT for:

- Private value transfer with maximum anonymity
- Personal financial privacy protection
- Censorship-resistant payments
- Store of value with quantum-resistant security

14.2 Financial Institutions

Banks and financial institutions can leverage NCRYPT for:

- Regulatory-compliant private transactions through accountable mode
- AML/KYC compliance while preserving user privacy
- Settlement and clearing with selective transparency
- Future-proof infrastructure resistant to quantum threats

14.3 Enterprises

Businesses can utilize NCRYPT for:

- Supply chain payments with appropriate privacy levels
- B2B transactions with selective auditability
- Confidential business transactions
- Long-term asset protection against quantum threats

14.4 Regulated Industries

Industries requiring compliance can benefit from:

- Healthcare: Private patient data transactions with auditability
- Legal: Confidential client transactions with regulatory compliance
- Government: Transparent public spending with private citizen data
- Financial Services: Compliant DeFi with privacy preservation

15. Conclusion

NCRYPT represents a fundamental advancement in blockchain technology, addressing critical challenges facing the cryptocurrency ecosystem: quantum vulnerability, privacy limitations, and regulatory compliance. By combining post-quantum cryptography with a flexible, multi-tier privacy framework, NCRYPT creates a blockchain platform that is secure against future threats while accommodating diverse user needs.

The DAPOA framework enables mathematically provable privacy guarantees while supporting selective disclosure for compliance, solving the long-standing tension between privacy advocates and regulatory requirements. This unique capability positions NCRYPT as the first blockchain that can simultaneously preserve user anonymity and meet institutional compliance needs.

As quantum computing advances toward breaking classical cryptography, the transition to post-quantum systems becomes increasingly urgent. NCRYPT provides a future-proof foundation for secure, private, and compliant digital value exchange in the quantum era.

The project's comprehensive roadmap outlines a clear path from initial development through mainnet launch and future expansion. With strong technical foundations, innovative privacy capabilities, and a focus on regulatory compliance, NCRYPT is positioned to become the infrastructure for secure digital value exchange in the quantum era.

NCRYPT invites developers, researchers, institutions, and privacy advocates to join in building a secure, private, and compliant blockchain ecosystem that stands the test of time—both classical and quantum.

16. References

16.1 Cryptographic Standards

• NIST Post-Quantum Cryptography Standardization: https://csrc.nist.gov/Projects/post-quantum-cryptography

• Module-LWE and Module-SIS Hardness Assumptions: Various academic papers on lattice-based cryptography

• Zero-Knowledge Proofs: Original papers by Goldwasser, Micali, and Rackoff

16.2 Privacy Technologies

• Ring Signatures: Original work by Rivest, Shamir, and Tauman

• Homomorphic Commitments: Pedersen commitments and variants

• Stealth Addresses: Concepts from Monero and Bitcoin privacy research

16.3 Blockchain Research

• Bitcoin Whitepaper: Nakamoto, S. (2008)

• Zcash Protocol: Zerocash Protocol Specification

• Monero Research Lab: Various privacy research papers

16.4 Quantum Computing

• Shor's Algorithm: Shor, P. W. (1994). "Algorithms for quantum computation: discrete logarithms and factoring"

• Grover's Algorithm: Grover, L. K. (1996). "A fast quantum mechanical algorithm for database search"

• Quantum Threat Assessment: Various NIST and academic publications

17. Glossary

17.1 Technical Terms

DAPOA:
Decentralized Anonymous Payment with Optional Accountability. NCRYPT's privacy framework enabling provable anonymity with selective disclosure.

Module-LWE:
Module Learning With Errors. A lattice-based cryptographic problem providing quantum-resistant security assumptions.

Module-SIS:
Module Short Integer Solution. A lattice-based cryptographic problem used for hash functions and commitments.

TXO:
Transaction Output. Unspent outputs that can be used as inputs in future transactions.

Zero-Knowledge Proof:
A cryptographic proof that demonstrates knowledge of a value without revealing the value itself.

Homomorphic Commitment:
A cryptographic commitment scheme that allows computations on committed values without revealing them.

Ring Signature:
A signature scheme that signs on behalf of a group, hiding the actual signer among group members.

17.2 Privacy Terms

Anonymity:
The inability to identify the sender or receiver of a transaction.

Unlinkability:
The inability to link multiple transactions to the same user.

Untraceability:
The inability to trace transaction histories through the blockchain.

Accountability:
The ability to selectively disclose transaction details to authorized parties for compliance.