Zytex Whitepaper

"The Next Generation Blockchain"

Introduction

Zytex is an innovative cryptocurrency forked from Xelis, designed to usher in a new era of privacy, scalability, and ease of use. Leveraging the foundational technologies of Xelis, Zytex integrates advanced features such as BlockDAG, Homomorphic Encryption, and Smart Contracts to deliver a robust and user-friendly blockchain platform.

Overview of Zytex

Zytex employs a Proof-of-Work (PoW) consensus mechanism over a BlockDAG (Directed Acyclic Graph) architecture, enabling high scalability and security. The integration of Homomorphic Encryption ensures the privacy of transactions and balances, while Smart Contracts provide a versatile environment for decentralized applications (dApps).

Key Objectives

Main Objectives:

1. **Privacy:** Preserve user privacy with encrypted transactions and balances.
2. **Smart Contracts:** Enable the execution of complex smart contracts.
3. **Scalability:** Utilize BlockDAG to support high transaction throughput and reduced confirmation times.
4. **Developer-Friendly:** Offer comprehensive tools and documentation for easy integration.

Additional Objectives:

1. **Custom Assets:** Allow the issuance of custom assets identical to the native Zytex (ZTX).
2. **Mining Accessibility:** Design the PoW algorithm to be friendly for both CPU and GPU miners.
3. **Decentralization:** Promote a decentralized network structure.
4. **User Simplicity:** Ensure the platform is easy to use for both end-users and developers.

Network Specifications

- Coin Name: Zytex (ZTX)
- Average Block Time: 15 seconds
- Maximum Block Size: 1.25 MB
- Block Reward: Approximately 1.46 ZTX
- Maximum Supply: 18.4 million ZTX
- Minimum Transaction Fees: 0.0001 ZTX per kB
- Atomic Units: 8
- Block Dev Fee: 10%

Technical Architecture

BlockDAG

BlockDAG enhances scalability and security by allowing multiple chains to run in parallel. Each block can have multiple parents, reducing the rate of orphaned blocks and improving overall network efficiency.

1. **Orphan Block Reduction:** Multiple blocks can be included in the DAG even if mined simultaneously.
2. **Non-Unique Height:** Blocks can share the same height.
3. **Topological Height:** Unique height ordered by the DAG.
4. **Stable Height:** Last height where DAG order cannot change.
5. **Block Types:** Sync, Side, and Orphaned blocks with specific rules and rewards.

Client Protocol

The Client Protocol allows multiple occurrences of the same transaction (TX) within different blocks, executing each TX only once based on the DAG's topological order. This prevents double-spending and reduces orphaned blocks.

Homomorphic Encryption

Zytex uses the ElGamal cryptosystem over the Ristretto255 curve to provide homomorphic properties, ensuring encrypted balances and transactions while maintaining privacy.

1. **Additive and Subtractive Operations:** Perform operations on ciphertexts without decryption.

2. **Enhanced Security:** Homomorphic properties support secure computation on encrypted data.

Zero-Knowledge Proofs (ZK Proofs)

Zytex employs ZK Proofs to validate encrypted transaction amounts, ensuring they do not exceed the sender’s balance and remain non-negative.

- **Bulletproofs:** Optimized for fast verification, allowing efficient range proofs.

P2P Encrypted Network

Zytex's peer-to-peer network uses ChaCha20-Poly1305 encryption to secure all communications, ensuring privacy and resistance to traffic analysis.

- **Decentralized and Lightweight:** Designed for low-resource devices while maintaining robust security.

Smart Contracts

Future updates will introduce Smart Contracts using the Zytex Virtual Machine (ZVM), allowing decentralized applications to leverage Zytex's secure and scalable infrastructure.

Key Features:

BlockDAG

1. **Scalability:** Supports multiple chains running in parallel, enhancing transaction throughput.
2. **Reduced Orphan Rate:** Multiple blocks can be included in the DAG even if mined simultaneously.
3. **Unique Heights:** Topological height orders blocks uniquely within the DAG.
4. **Stable Height:** Ensures the order of blocks cannot change past a certain height.

Homomorphic Encryption

1. **Privacy:** Ensures transactions and balances remain confidential.
2. **Secure Computation:** Allows operations on encrypted data without revealing underlying information.
3. **ElGamal Cryptosystem:** Utilizes the Ristretto255 curve for robust security.

Zero-Knowledge Proofs

1. **Validation:** Verifies encrypted transaction amounts without revealing them.
2. **Bulletproofs:** Provides efficient range proofs for fast verification.

P2P Network

1. **Encryption:** Uses ChaCha20-Poly1305 for secure communication.
2. **Decentralization:** Eliminates single points of failure, enhancing security.
3. **Lightweight:** Designed for use on low-resource devices.

Future Directions

Zytex aims to continually evolve, with planned enhancements including:

1. **New PoW Algorithm:** To improve mining efficiency and security.
2. **Smart Contract Integration:** Enabling a robust ecosystem for dApps.
3. **Confidential Assets:** Allowing decentralized tokens with privacy features akin to native ZTX.

Conclusion

Zytex builds on the innovative framework of Xelis, introducing enhancements that make it a formidable player in the blockchain space.

With its focus on privacy, scalability, and ease of use, Zytex is set to drive the next wave of cryptocurrency adoption and innovation.