DAPA Whitepaper

Homomorphic Encrypted Blockchain

DAPA - A Private BlockDAG
with Social Contracts

Introduction

DAPA is an Advanced Layer-1 Blockchain cryptocurrency using code developed by Slixe and Devs, its been designed to usher in a new era of Total user Security and Privacy for all Crypto transaction payments and decentalized applications giving a corporate scalability with ease of use. **DAPA** uses Homomorphic Encryption, and Smart Contracts to deliver a robust and user-friendly blockchain Payment platform to its users.

DAPA Overview

DAPA employs a Proof-of-Work (PoW) consensus mechanism over a BlockDAG (Directed Acyclic Graph) architecture, enabling a high level of scalability and security. The integration of Homomorphic Encryption ensures the privacy of transactions and balances. Traditional public digital ledgers offer transparency, but they often compromise user privacy by exposing wallet balances and transaction details DAPA addresses this problem with its Homomorphic encryption without sacrificing the blockchain's speed or scalability with Smart Contracts providing a Secure development environment for decentralized applications (dApps).

DAPA 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 DAPA Asset.
2. **Mining Accessibility:** The algorithm is Design for PoW to be friendly to both CPU and GPU miners.
3. **Decentralization:** Promoting a decentralized network structure.
4. **User Simplicity:** Ensure the platform is easy to use for both end-users and developers.

DAPA Specifications

Coin Name: DAPA Average Block Time: 15 seconds Maximum Block Size: 1.25 MB Block Reward: Approximately 7.49 DAPA Maximum Supply: 800 million DAPA Minimum Transaction Fees: 0.0001 DAP per kB Atomic Units: 8 Block Dev Fee: 0%

DAPA Technical

The 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

DAPA uses the provenElGamal cryptosystem over the Ristretto255 curve to provide homomorphic properties, ensuring encrypted balances and transactions while maintaining totaly private.

1. **Additive and Subtractive Operations:** Perform operations on ciphertexts without decryption.
2. **Enhanced Security:** Homomorphic properties support secure computation on encrypted data without the need for decryption.
   This means that operations can be performed directly on encrypted data and when decrypted the results will reflect the outcome of the same operations as if they had been carried out on the original unencrypted data.
   This provides for a totaly secure and private ecosytem and means only the parties involved can access the values.

Zero-Knowledge Proofs (ZK Proofs)

DAPA employs ZK Proofs to validate encrypted transaction amounts, ensuring they do not exceed the sender's balance and remain non-negative.
zero-knowledge proofs are crucial for validating transactionson the DAPA blockchain involving encrypted data. Specifically we use ZKPs to confirm the validity of ciphertexts—encrypted representations of amounts transferred.

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

P2P Encrypted Network

DAPA 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

Smart Contracts: As we go forward updates will introduce Smart Contracts using the DAPA Virtual Machine (DVM), allowing decentralized applications to leverage **DAPA**s fast,secure and Corporately scalable infrastructure for Decentralized applications (**DAPPS**).

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 values without revealing the transaction data.
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 in developing countries where reception can be very slow.

Future Directions

DAPA will continually grow, 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 DAPA Asset.

DAPA Objectives

DAPA Is an initiative that works in the new emerging Zero energy field we intend to provide Zero Energy Power units for the use of households and Busineses.
The units will be supplied by our company on a payment lease maintainance contract, The units will supply all electrical
energy Requirments to households without recourse to the national grid.
The payment threshold will be very low compared to todays exhorbitant energy prices estimates are 95% lower than Electric and Gas bills for an average month usage.
This makes Electrical Boiler installation a reality for all households and Busineses Today.

DAPA

For its next phase, DAPA will be looking at introducing to the market a vehicle that requires no Batteries to run, produces its own electrical needs with spare capacity to provide an electrical supply to Properties that are either not on the grid, or would just like there own power supply without the need for Unrecyclable wind turbines and solar panels.

GREEN ENERGY SUPPORTERS

You Now Have the Chance to Save the Planet by supporting DAPA with it's move to True Green FREE ENERGY SUPPLIES for all Citizens of Earth
By Supporting those working on your behalf to move away from Fossil Fuels to Free Zero Energy supplies necessary to stop harming the planet we all inhabit, we all feel there is nothing we can do as individuals, so here's your chance to Join and support us at DAPA with our Coin offer, start from as little as **$3.00** that's all it takes to help our fight.
God bless all of you who see your way to support this initiative.

Representation of Batteryless vehicle chasis that may be used for Production