RONAN HENRIQUES
PRAKAMYA JOSHI
AARYAN AGARWAL
ANAND SINHA

BIT N BUILD 2025

HACKATHON

TEAM GREEN DRAGON

BLOCKCHAIN ENCRYPTION IN JAVA

Traditional data systems are centralized and prone to tampering. Our blockchain ensures decentralized, tamper-proof, cryptographically secure transactions.

WHAT IS A BLOCKCHAIN ?

A blockchain is basically a distributed database, where data is stored in blocks linked together in a chronological chain. Each block contains transaction details, a timestamp, and a unique cryptographic hash, which ensures the integrity and security of the data.

Distributed Ledger

- all participants (nodes) in the network have an up-to-date, synchronized copy of all transactions; ensures transparency and prevents any single authority from controlling or altering the record independently.

Consensus Mechanism

- algorithms like Proof of Work or Proof of Stake, guaranteeing that only legitimate transactions are recorded and that the network remains consistent and secure.

Immutability and Security

- Once data is added to the blockchain, it cannot easily be changed or deleted. Security is further reinforced through cryptographic methods.

WHY OUR BLOCKCHAIN?

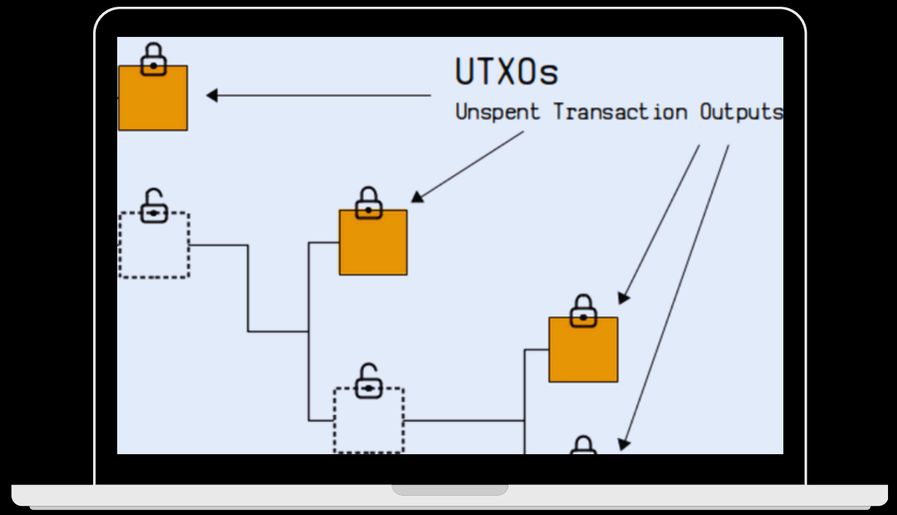
For any transaction;
integrity, efficiency, security, and future-proofing are important.

Pillars of Our Blockchain :-

- UTXO Model → Prevents double spending
- Merkle Root → Efficient transaction verification
- Proof-of-Work → Tamper-resistance & security
- Lattice encryption → Provides post-quantum security

UTXO MODEL

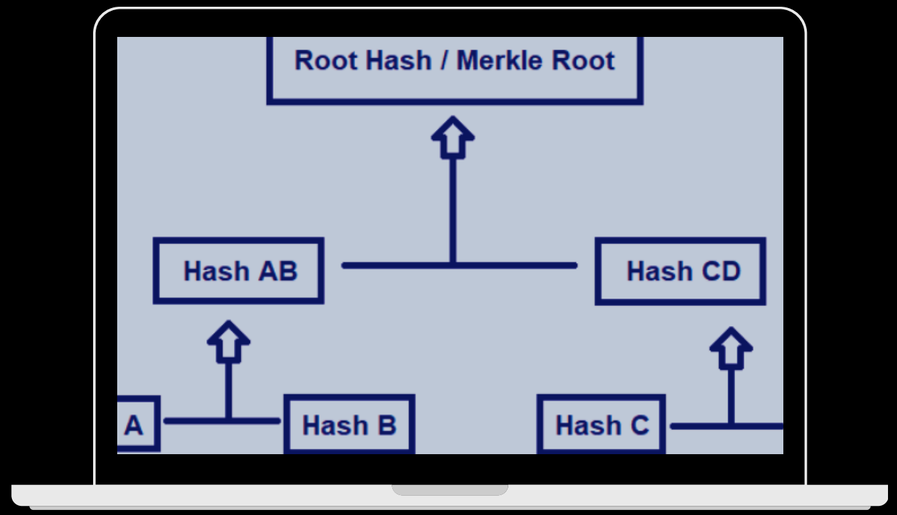
In our blockchain, every transaction must point to a valid unspent transaction output. This ensures coins can’t be copied or reused. It’s the same model that Bitcoin itself uses.



- Coins are tracked as unspent outputs of previous transactions.
- Each transaction consumes UTXOs and creates new ones.
- Prevents double-spending automatically.

MERKLE ROOT

This gives us scalability. If a mobile user wants to verify their transaction, they don’t need the entire blockchain, just a proof from the Merkle tree. It’s efficient and future-proof.



- All transactions are hashed into a Merkle Tree.
- The Merkle Root becomes the block’s fingerprint.
- Enables lightweight proofs without downloading the full chain.

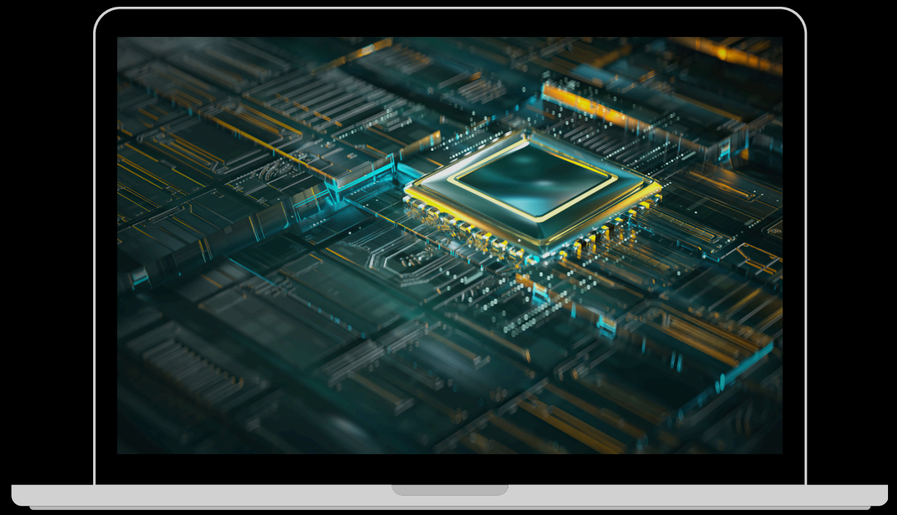
POWER OF WORK MODEL

In Bitcoin, mining a block takes ~10 minutes because of very high difficulty. That’s not practical for a hackathon demo. So we built adjustable difficulty low enough to mine blocks live, but high enough to still prove security. This makes our blockchain a scalable demo platform for real-world concepts.

- **Blocks mined by solving a cryptographic puzzle.**
- **Hash must start with difficulty number of zeros.**
- **Makes altering past data computationally infeasible.**

LATTICE ENCRYPTION

Unlike RSA or ECC, lattice-based cryptography is secure against both classical and quantum computers. It provides a future-proof foundation for blockchain.



- **Efficient even on constrained devices.**
- **Ensures long-term viability.**
- **Homomorphic and zero-knowledge features from lattice cryptography can enhance privacy without sacrificing trust.**

WHY LATTICE ENCRYPTION?

Most conventional encryption schemes rely on problems that are hard for classical computers but easy for quantum ones:

- **RSA(Rivest-Shamir-Adleman) depends on the difficulty of factoring large integers.**
- **ECC (Elliptic Curve Cryptography) relies on solving discrete logarithms over elliptic curves.**

These are vulnerable to Shor's algorithm, which runs efficiently on quantum computers and can break these systems in polynomial time. That means once quantum machines scale up, your blockchain's security will be nullified.

1. Quantum Resistance

Lattice problems like SVP and LWE remain hard even for quantum algorithms.

2. Efficiency & Speed

Many lattice schemes (e.g., NTRU, Kyber) offer faster key generation and encryption/decryption than RSA.
They also support smaller key sizes for equivalent security, which is great for bandwidth-sensitive blockchain nodes.

3. Advanced Features

Homomorphic encryption: You can perform computations directly on encrypted data—ideal for privacy-preserving smart contracts.
Digital signatures: Schemes like Dilithium offer fast, secure signing for blockchain transactions.

4. Real-World Blockchain Use

Lattice encryption is already being explored for quantum-safe cryptocurrencies, secure consensus protocols, and privacy-preserving ledgers.

FEATURES IMPLEMENTED

1. Block Structure → Each block stores data, its hash, and previous hash.
2. Chaining of Blocks → Each block links securely to the previous block.
3. SHA-256 Hashing → Ensures immutability of data.
4. Proof-of-Work Mining → Adjust difficulty to simulate real blockchain mining.
5. Blockchain Validation → Detects tampering instantly.
6. JSON Output (via Gson) → Easy to visualize the blockchain.

PROCESS

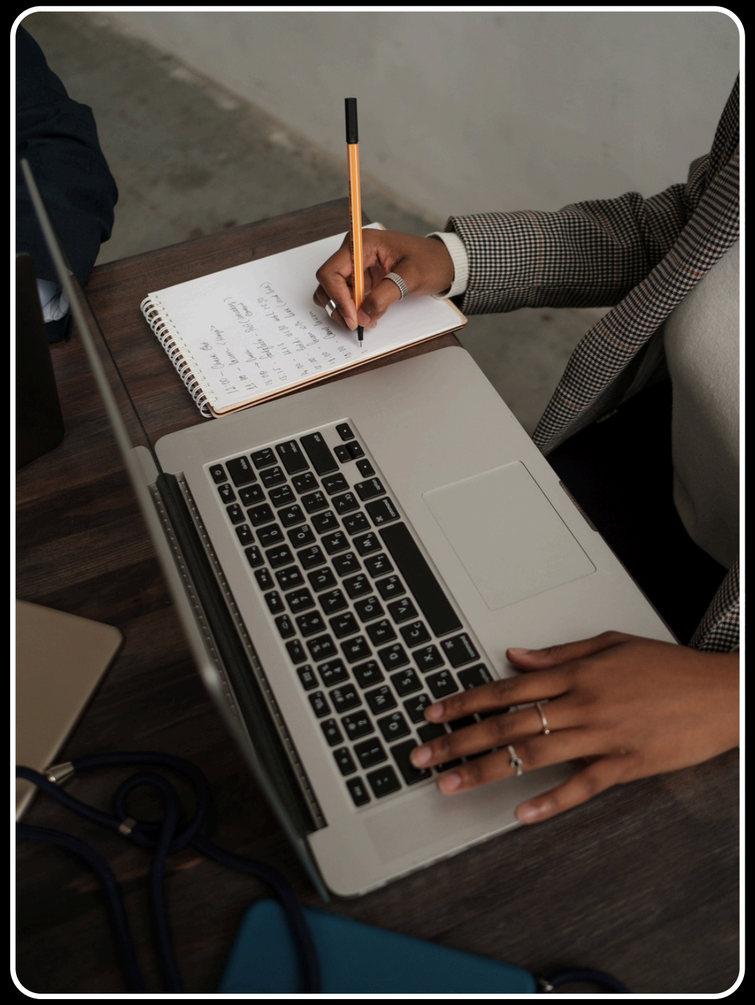
- Create a genesis block (first block).
- Add new blocks → each block references previous block’s hash.
- Use Proof-of-Work (mining) → find hash starting with N zeros.
- Verify chain → check hashes + links.
- Print blockchain in JSON format.

FUTURE IMPROVEMENTS

- Add Transactions instead of simple strings.
- Implement Digital Signatures (ECDSA) for security.
- Replace array with Merkle Trees for efficient storage.
- Build a P2P Network to simulate multiple nodes.
- Add a simple wallet system.
- Faster consensus (instead of PoW).
- A simple web explorer.
- A unique application domain (supply chain, credentials, etc.

CONCLUSIONS

In traditional transactions: Only the bank or payment processor verifies the transaction, while in blockchain: Everyone in the network verifies it. The puzzle ensures that adding a block takes effort, which prevents spam or cheating. Blockchain integration in finance enhances transparency, reduces fraud, and lowers transaction costs by removing intermediaries. It enables faster cross-border payments, secure digital identities, and real-time settlement, transforming traditional banking into a more efficient and trustworthy system.



what sets us apart?

- Demo-friendly yet secure.
- Educational + easy to understand.
- Extendable to micropayments, tokens, IoT, mobile apps.

THANK YOU FOR YOUR ATTENTION

Our blockchain project is About showing how the very same principles that power Bitcoin and Ethereum can be simplified, demonstrated, and extended into real-world applications. With UTXO for integrity, Merkle roots for scalability, and Proof-of-Work for security, we’ve built a strong foundation that is both educational and innovative.