23. Perform Privacy-Preserving Atomic Swaps with BTC Using Taproot HTLCs in JavaScript

Why: Taproot's script efficiency enables cross-chain HTLCs (Hashed Timelock Contracts) with reduced reveal risk. This hack allows swapping BSTY for BTC privately, useful in 2026 for diversifying holdings without KYC exchanges, preserving user anonymity.

How to Implement: Set up HTLC on both chains; use same preimage. Coordinate off-chain; claim with reveal or refund via timelock.

```
javascript
const crypto = require('crypto');

// Hack: Taproot HTLC for atomic swap
function createHTLC(preimage, recipientPubkey, timeout) {
    const hash = crypto.createHash('sha256').update(preimage).digest('hex');
    // Script: OP_IF <hash> OP_EQUALVERIFY <recipient> OP_CHECKSIG OP_ELSE <timeout>
OP_CHECKLOCKTIMEVERIFY OP_DROP <refund> OP_CHECKSIG OP_ENDIF
    const taprootScript = `Taproot tree with HTLC branches`;  // Encode
    return { address: 'gb1q...htlc', hash };
}

function claimSwap(txid, preimage) {
    // Build spend tx revealing preimage
    return 'signed_tx_hex';  // Broadcast to BSTY
}

const preimage = 'secret';
const htlc = createHTLC(preimage, 'recipient_pub', 144);  // 24h timeout
console.log(htlc);
```

Analysis: Atomicity ensures no counterparty risk; Taproot hides HTLC until claim, reducing front-running. BSTY-BTC swaps settle in minutes due to fast blocks, boosting privacy by obfuscating cross-chain flows in 2026's monitored ecosystems.