WATTx Technical Architecture Overview

Version: 0.1.7-dev **Date:** January 27, 2026

Executive Summary

WATTx is a hybrid PoW/PoS blockchain combining:

- **Multi-chain merged mining** (Monero, Bitcoin, Litecoin, etc.)
- **Monero-style UTXO privacy** (ring signatures, stealth addresses)
- **EVM-based cross-chain privacy pools** for anonymous stablecoin transfers
- **QTUM-based architecture** with both UTXO and EVM layers

---

1. Multi-Chain Merged Mining Architecture

1.1 Overview

WATTx supports merged mining with multiple parent chains simultaneously, allowing miners to earn WATTx rewards while mining other cryptocurrencies.

```
┌─────────────────────────────────────────────────────────────────┐
│                    PARENT CHAINS                                │
│                                                                 │
│  ┌──────────┐  ┌──────────┐  ┌──────────┐  ┌──────────┐         │
│  │  Monero  │  │ Bitcoin  │  │ Litecoin │  │   Dash   │         │
│  │ RandomX  │  │ SHA256d  │  │  Scrypt  │  │   X11    │         │
│  └────┬─────┘  └────┬─────┘  └────┬─────┘  └────┬─────┘         │
│       │             │             │             │               │
│       └─────────────┴──────┬──────┴─────────────┘               │
│                            │                                    │
│                     ┌──────▼──────┐                             │
│                     │  WATTx      │                             │
│                     │ AuxPoW Node │                             │
│                     └─────────────┘                             │
│                                                                 │
└─────────────────────────────────────────────────────────────────┘
```

1.2 Supported Algorithms

Parent Chain	Algorithm	Stratum Port	Status
Monero	RandomX	3337	Implemented
Bitcoin	SHA256d	3338	Implemented
Litecoin	Scrypt	3339	Planned
Dash	X11	3340	Planned
Kaspa	kHeavyHash	3341	Planned

1.3 Merged Mining Flow

1. **Miner connects** to WATTx merged stratum server
2. **Server fetches** block templates from both parent chain and WATTx
3. **WATTx block hash** embedded in parent chain's coinbase/extra nonce
4. **Miner submits** solution to parent chain
5. **If hash meets WATTx target**, construct AuxPoW proof and submit WATTx block

6. **Miner earns** both parent chain and WATTx rewards

1.4 Key Files

```
src/stratum/
├── stratum_server.h/cpp       # Direct XMRig stratum
├── merged_stratum.h/cpp       # Monero merged mining
├── multi_merged_stratum.h/cpp # Multi-chain support
├── parent_chain.h             # Parent chain interface
├── parent_chain_bitcoin.h     # Bitcoin specifics
└── parent_chain_monero.h      # Monero specifics

src/rpc/stratum_rpc.cpp        # RPC commands
```

1.5 RPC Commands

```bash
# Start Monero merged mining
wattx-cli startmergedstratum 3337 "127.0.0.1" 18081 "MoneroAddr" "WATTxAddr"

# Start Bitcoin merged mining
wattx-cli startbitcoinmergedstratum 3338 "127.0.0.1" 8332 "user" "pass" "WATTxAddr"

# Check stratum status
wattx-cli getstratuminfo
```

---

2. UTXO Privacy Layer (Monero-Style)

2.1 Privacy Features

WATTx native chain implements Monero-inspired privacy:

Feature	Description	Status
Ring Signatures	Hide sender among decoys	Planned
Stealth Addresses	One-time recipient addresses	Planned
RingCT	Confidential transaction amounts	Planned
Bulletproofs	Efficient range proofs	Planned

2.2 Architecture

```
┌─────────────────────────────────────────────────────────────────┐
│                   WATTx UTXO Layer                              │
│                                                                 │
│  ┌─────────────┐  ┌─────────────┐  ┌─────────────────────────┐  │
│  │    Ring     │  │  Stealth    │  │    Confidential         │  │
│  │  Signatures │  │ Addresses   │  │    Transactions         │  │
│  │             │  │             │  │                         │  │
│  │ - Decoy set │  │ - One-time  │  │ - Hidden amounts        │  │
│  │ - Key image │  │   keys      │  │ - Pedersen commits      │  │
│  │ - MLSAGs    │  │ - View keys │  │ - Range proofs          │  │
│  └─────────────┘  └─────────────┘  └─────────────────────────┘  │
│                                                                 │
│                         ┌─────────────┐                           │
│                         │ Block Reward│                           │
│                         │  (Shielded) │                           │
│                         └─────────────┘                           │
└──────────────────────────────────────────────────────────────────┘
```

2.3 Block Rewards

Mining and staking rewards are issued as shielded outputs:

- Miner/Staker provides stealth public key
- Reward UTXO created with that key
- Only key holder can spend

---

3. EVM Cross-Chain Privacy Pools

3.1 Overview

Privacy pools enable anonymous cross-chain stablecoin transfers:

- **Deposit** USDT on any chain (ETH, BSC, Polygon, Altcoinchain)
- **Hold** privately as shielded balance on WATTx
- **Withdraw** to ANY chain with no traceable link to deposit

3.2 Architecture

```
┌──────────────────────────────────────────────────────────────────────────────┐
│                           EXTERNAL CHAINS                                     │
│                                                                              │
│  ┌───────────┐  ┌───────────┐  ┌───────────┐  ┌───────────┐  ┌───────────┐  │
│  │ Ethereum  │  │    BSC    │  │  Polygon  │  │Altcoinchain│  │ Arbitrum  │  │
│  │ PrivacyPool│  │ PrivacyPool│  │ PrivacyPool│  │ PrivacyPool│  │ PrivacyPool│  │
│  │  (USDT)   │  │  (USDT)   │  │  (USDT)   │  │  (USDT)   │  │  (USDT)   │  │
│  │  chainId:1 │  │ chainId:56 │  │chainId:137 │  │chainId:2330│  │chainId:42161│
│  └─────┬─────┘  └─────┬─────┘  └─────┬─────┘  └─────┬─────┘  └─────┬─────┘  │
│        │              │              │              │              │         │
│        └──────────────┴──────────────┴───────┬──────┴──────────────┘         │
│                                              │ LayerZero / Bridge             │
└──────────────────────────────────────────────┼───────────────────────────────┘
                                               │
                                               ▼
┌──────────────────────────────────────────────────────────────────────────────┐
│                           WATTx EVM                                            │
│                                                                              │
│  ┌─────────────────────────────────────────────────────────────────────────┐  │
│  │                      PrivacyController                                    │  │
│  │                                                                         │  │
│  │  ┌────────────────┐  ┌────────────────┐  ┌──────────────────────┐      │  │
│  │  │  Merkle Tree   │  │  ZK Verifier   │  │  Chain Registry      │      │  │
│  │  │  Commitments   │  │  Groth16 Proofs │  │  Liquidity Tracking  │      │  │
│  │  │  (20 levels)   │  │                │  │                      │      │  │
│  │  └────────────────┘  └────────────────┘  └──────────────────────┘      │  │
│  └─────────────────────────────────────────────────────────────────────────┘  │
└──────────────────────────────────────────────────────────────────────────────┘
```

3.3 Privacy Flow

Deposit Flow

```
User (Ethereum)                    PrivacyPool (ETH)              WATTx Controller
      │                                  │                               │
      |  1. Approve USDT                 |                              |
      |─────────────────────────────────>|                              |
      |                                  |                              |
      |  2. deposit(amount, stealthKey)  |                              |
      |─────────────────────────────────>|                              |
      |                                  |                              |
      |                                  |  3. Lock USDT in pool        |
      |                                  |                              |
      |                                  |  4. Cross-chain message      |
      |                                  |─────────────────────────────>|
      |                                  |                              |
      |                                  |                              |  5. Add commitment
      |                                  |                              |     to Merkle tree
      |                                  |                              |
      |<─────────────────────────────────────────────────────────────────|
      |  6. User has shielded balance                                   |
```

Withdrawal Flow

```
User                               WATTx Controller              PrivacyPool (BSC)
  |                                      |                              |
  |  1. Generate ZK proof (off-chain)    |                              |
  |     - Proves commitment exists       |                              |
  |     - Proves nullifier correct       |                              |
  |     - Hides WHICH commitment         |                              |
  |                                      |                              |
  |  2. withdraw(proof, nullifier, etc.) |                              |
  |─────────────────────────────────────>|                              |
  |                                      |                              |
  |                                      |  3. Verify ZK proof          |
  |                                      |  4. Mark nullifier used      |
  |                                      |                              |
  |                                      |  5. Cross-chain message      |
  |                                      |─────────────────────────────>|
  |                                      |                              |
  |                                      |                              |  6. Release USDT
  |<───────────────────────────────────────────────────────────────────|
  |  7. Receive USDT on BSC (anonymous)                                |
```

3.4 Smart Contracts

Contract	Chain	Purpose
`PrivacyPoolStandalone.sol`	Each external chain	Hold USDT, process deposits/withdrawals
`PrivacyController.sol`	WATTx EVM	Manage commitments, verify proofs
`MerkleTree.sol`	WATTx EVM	Store commitment tree
`MockVerifier.sol`	Testing	Mock ZK verification

3.5 Fixed Denominations

For maximum anonymity, deposits use fixed amounts:

Denomination	USDT Amount	Anonymity Set

DENOM_100	100 USDT	Large
DENOM_1000	1,000 USDT	Medium
DENOM_10000	10,000 USDT	Medium
DENOM_100000	100,000 USDT	Smaller

3.6 Contract Deployment

```bash
# Altcoinchain (chainId: 2330)
# RPC: https://alt-rpc2.minethepla.net

cd contracts/privacy
npm install
npx hardhat compile
npx hardhat run scripts/deploy.js --network altcoinchain
```

---

4. Combined System Overview

```
┌─────────────────────────────────────────────────────────────────────────────┐
│                             WATTx ECOSYSTEM                                 │
│                                                                             │
│  ┌──────────────────────────────────────────────────────────────────────┐   │
│  │                       CONSENSUS LAYER                                │   │
│  │                                                                      │   │
│  │   ┌─────────────┐         ┌─────────────┐         ┌─────────────┐    │   │
│  │   │   Merged    │         │   X25X      │         │   PoS       │    │   │
│  │   │   Mining    │    +    │ Multi-Algo  │    +    │  Staking    │    │   │
│  │   │  (AuxPoW)   │         │  Mining     │         │             │    │   │
│  │   └─────────────┘         └─────────────┘         └─────────────┘    │   │
│  │                                                                      │   │
│  └──────────────────────────────────────────────────────────────────────┘   │
│                                    │                                        │
│                                    ▼                                        │
│  ┌──────────────────────────────────────────────────────────────────────┐   │
│  │                        WATTx BLOCKCHAIN                              │   │
│  │                                                                      │   │
│  │   ┌─────────────────────────┐    ┌─────────────────────────────┐     │   │
│  │   │      UTXO LAYER         │    │        EVM LAYER            │     │   │
│  │   │                         │    │                             │     │   │
│  │   │ • Ring Signatures       │    │ • Privacy Pools             │     │   │
│  │   │ • Stealth Addresses     │    │ • Smart Contracts           │     │   │
│  │   │ • Confidential TX       │    │ • DeFi Applications         │     │   │
│  │   │ • Native Currency       │    │ • Cross-chain Bridge        │     │   │
│  │   │                         │    │                             │     │   │
│  │   └─────────────────────────┘    └─────────────────────────────┘     │   │
│  │                                                                      │   │
│  └──────────────────────────────────────────────────────────────────────┘   │
│                                    │                                        │
│                                    ▼                                        │
│  ┌──────────────────────────────────────────────────────────────────────┐   │
│  │                      CROSS-CHAIN LAYER                               │   │
│  │                                                                      │   │
│  │    ┌──────────┐  ┌──────────┐  ┌──────────┐  ┌──────────┐             │   │
│  │    │ Ethereum │  │   BSC    │  │ Polygon  │  │Altcoinchain│           │   │
│  │    │   Pool   │  │   Pool   │  │   Pool   │  │   Pool   │             │   │
│  │    └──────────┘  └──────────┘  └──────────┘  └──────────┘             │   │
│  │                                                                        │   │
│  └───────────────────────────────────────────────────────────────────────┘   │
│                                                                               │
└──────────────────────────────────────────────────────────────────────────────┘
```

5. Key Technical Details

5.1 Merkle Tree

- **Levels:** 20 (supports ~1M commitments)
- **Hash:** Keccak256 (Poseidon for ZK circuits)
- **Root History:** 100 roots kept for verification flexibility

5.2 ZK Proofs

- **System:** Groth16 (via snarkjs/circom)
- **Proof Size:** 8 uint256 values
- **Public Inputs:** Root, Nullifier, Amount, Recipient

5.3 Fees

Operation	Fee
Deposit	0.1% (configurable, max 1%)
Withdrawal	0.1% (configurable, max 1%)
Cross-chain	LayerZero gas fees

6. Deployment Status

Altcoinchain (chainId: 2330)

Component	Address	Status
RPC Endpoint	https://alt-rpc2.minethepla.net	Active
PrivacyPoolStandalone	TBD	Ready to deploy
MockVerifier	TBD	Ready to deploy
MockUSDT	TBD	Ready to deploy

WATTx

Component	Status
Merged Mining (Monero)	Implemented
Merged Mining (Bitcoin)	Implemented
UTXO Privacy	Planned
EVM Privacy Controller	Ready

7. Future Roadmap

1. **Q1 2026:** Deploy privacy pools to Altcoinchain and testnets
2. **Q2 2026:** Implement ZK circuits (circom) for production
3. **Q3 2026:** UTXO privacy layer (ring signatures, stealth addresses)
4. **Q4 2026:** Full production deployment across all chains

---

8. References

- **Codebase:** `/home/nuts/Documents/WATTx/WATTx-0.1.7-dev/`
- **Contracts:** `/contracts/privacy/`
- **Stratum:** `/src/stratum/`
- **Altcoinchain:** `/home/nuts/Documents/go-altcoinchain_FUSAKA/`

Document generated: January 27, 2026