MYT

A Privacy-Preserving Settlement Layer for Machines, AI Agents, and Enterprises

Technical Specification & Architecture

Version 1.0 — Final Release

Abstract

Modern digital economies increasingly depend on autonomous software systems, artificial intelligence agents, and distributed infrastructure. Yet existing financial networks remain fundamentally misaligned with machine-native settlement: they assume human oversight, tolerate surveillance, and offer no privacy guarantees for transacting parties.

MYT is a Proof-of-Work blockchain protocol designed as a privacy-preserving settlement layer for autonomous systems, individual users, and enterprise environments. Built on a CryptoNote-derived privacy architecture and secured by the RandomX mining algorithm, MYT combines cryptographically enforced transaction privacy with Bitcoin-style deterministic monetary policy and decentralized network security.

The protocol prioritizes technical stability, deterministic behavior, and long-term sustainability. Future development phases introduce selective disclosure proofs and a cryptographic machine identity layer, enabling verifiable settlement for autonomous software while preserving the privacy guarantees of the underlying network. MYT is designed to be foundational infrastructure — not a product.

1 Introduction

The emergence of autonomous software agents, machine learning systems, and distributed computation networks creates new requirements for financial infrastructure. These systems operate continuously, interact programmatically, and often require settlement across organizational or jurisdictional boundaries — without human intermediaries.

Existing blockchain infrastructure largely fails this use case. Transparent ledgers expose all transactional data to public surveillance. Centralized smart contract platforms introduce governance risk and points of censorship. Privacy-preserving alternatives either lack deterministic monetary policy or are not designed with machine-compatibility as a primary objective.

MYT addresses both the privacy deficit and the machine-compatibility gap by providing: strong cryptographic transaction privacy, open Proof-of-Work mining, a capped and predictable supply schedule, and a development roadmap targeting machine settlement infrastructure.

This document describes the technical specification of the MYT protocol — including consensus parameters, privacy mechanisms, monetary policy, and planned protocol extensions.

2 Problem Statement

2.1 Surveillance Finance

The majority of existing blockchain systems operate on fully transparent ledgers. All transaction inputs, outputs, amounts, and addresses are permanently visible to any observer. This design is incompatible with financial privacy as a baseline requirement — for individuals, enterprises, and autonomous systems alike.

2.2 Absence of Machine-Native Settlement

Autonomous software systems — AI agents, computation networks, automated service markets — require settlement infrastructure that operates without human oversight. Few privacy-preserving settlement layers have been designed with autonomous software systems as a primary use case.

2.3 Verification Without Disclosure

Enterprises and regulated environments require the ability to verify financial interactions without exposing full transactional history. Traditional privacy systems offer a binary choice: full transparency or complete opacity. Neither is sufficient for professional or regulatory contexts.

2.4 Centralization Risk

Many contemporary blockchain networks rely on delegated consensus, staking systems, or permissioned validator sets. These architectures introduce systemic governance risk and reduce resistance to censorship. Open Proof-of-Work consensus with an ASIC-resistant algorithm provides a more robust foundation.

3 Related Systems

MYT shares lineage with several existing protocols. This section briefly positions MYT relative to the most relevant systems.

Property	Bitcoin	Monero	Zcash	MYT
Transaction Privacy	No	Yes	Optional	Yes
ASIC-Resistant Mining	No	Yes	No	Yes
Fixed Supply Cap	Yes	No*	No*	Yes
No Tail Emission	Yes	No	No	Yes
Machine-Native Design	No	No	No	Yes
Selective Disclosure	No	Limited	Yes	Planned
Agent Identity Layer	No	No	No	Planned

** Monero and Zcash have tail emission schedules; their supplies are technically uncapped.*

Bitcoin established the fixed-supply PoW model and proved decentralized monetary policy is achievable. MYT inherits this monetary design directly. Bitcoin's transparent ledger is by design unsuitable for private settlement.

Monero is the most mature privacy-preserving PoW chain and the primary technical reference for MYT's privacy stack. MYT diverges in three ways: a fixed supply cap (no tail emission), a Bitcoin-style halving schedule, and an explicit design goal of machine-native settlement infrastructure.

Zcash introduced zk-SNARK-based privacy but relies on optional shielded transactions and a trusted setup. Its governance model and supply schedule differ materially from MYT's design goals.

Smart contract platforms (Ethereum and derivatives) provide programmability but expose all transaction data by default. Their account-based models require identity and registration that autonomous agents cannot easily satisfy without centralized infrastructure.

4 Design Principles

Core Design Principles

– Privacy by Default — Sender, receiver, and amount are always protected. Privacy is not opt-in.

– Decentralization — Proof-of-Work with ASIC-resistant algorithm ensures open participation.

– Deterministic Monetary Policy — Supply schedule is fixed, transparent, and unalterable.

– Infrastructure First — Technical correctness and long-term stability over speculative growth.

– Machine Compatibility — Extensions enable autonomous software to perform secure financial settlement.

– No Consensus-Level Identity — The blockchain remains a neutral settlement layer.

5 Network Architecture

MYT operates as a fully decentralized peer-to-peer network. Nodes maintain the blockchain, independently validate transactions and blocks, and propagate data without central coordination.

- Full nodes — Maintain the complete blockchain and enforce all consensus rules
- Mining nodes — Produce new blocks and secure the network through Proof-of-Work
- Remote RPC nodes — Provide API access for wallets and downstream services
- Light wallets — Connect to remote nodes without storing the full chain

Default Network Ports

Service	Default Port
P2P (node communication)	39080
RPC (API interface)	39081
ZMQ (event streaming)	39082

6 Consensus Mechanism

MYT uses Proof-of-Work consensus. Miners compete to find a valid solution to a cryptographic puzzle, producing new blocks. The chain with the greatest cumulative work is the canonical chain.

6.1 Mining Algorithm

MYT uses a staged mining algorithm schedule inherited from the CryptoNote hardfork plan. At network launch (HF1, block 1), the active proof-of-work algorithm is CryptoNight. The network transitions to RandomX at hardfork 12 (block 28,895).

Phase	Block Range	Algorithm
Launch – HF11	1 – 28,894	CryptoNight (variant per HF)
HF12+	28,895+	RandomX

CryptoNight is a memory-hard algorithm designed to be GPU- and ASIC-resistant. RandomX executes random programs on a virtual machine, making its workload resemble general-purpose CPU computation. Both algorithms favor commodity hardware and reduce mining centralization risk.

Mining Algorithm Transition

– HF1–HF11 (blocks 1–28,894): CryptoNight family — variant determined by block major version

– HF12 (block 28,895): RandomX activates — controlled by RX_BLOCK_VERSION=12 in consensus code

– Algorithm selection is automatic: block major_version ≥ 12 routes to RandomX, lower versions to CryptoNight

– Miners must update software at the HF12 transition; no action required before that point

6.2 Block Time

MYT targets a 60-second block production interval, providing fast confirmation, sufficient propagation time, and a clean basis for the emission schedule.

6.3 Hardfork Schedule

MYT uses a compressed hardfork schedule designed to bring the network to full protocol maturity quickly. All consensus upgrades — including RingCT, Bulletproofs, CLSAG, and RandomX — activate within the first ~32,000 blocks. Each hardfork activates new consensus rules at a predefined block height.

HF	Block Height	Key Changes
HF1	1	Genesis rules; CryptoNight PoW
HF2	23,135	Min mixin 2; dynamic outputs
HF3	23,711	Output amount rules
HF4	24,287	Dynamic fee model; TX v2
HF5	24,863	Consensus refinements

HF	Block Height	Key Changes
HF6	25,439	Min mixin 4; RingCT enforced
HF7	26,015	Min mixin 6; sorted inputs
HF8	26,591	Min mixin 10; Bulletproofs
HF9	27,167	Borromean range proofs banned
HF10	27,743	Bulletproof v2; long-term block weight
HF11	28,319	Bulletproof v2 enforced
HF12	28,895	RandomX activates; min 2 outputs
HF13	29,471	CLSAG ring signatures allowed
HF14	30,047	CLSAG enforced; old RCT types banned
HF15	30,623	Min mixin 15; Bulletproof+; view tags
HF16	31,199	Tagged-key outputs enforced
HF17	162,084	Strict 21,000,000 MYT emission cap enforced

The compressed schedule ensures the network reaches full protocol maturity (HF16) within approximately the first 31,199 blocks. All hardfork heights are defined in src/hardforks/hardforks.cpp.

7 Monetary Policy

MYT follows a deterministic emission schedule inspired by Bitcoin. The total supply is fixed, the issuance schedule is predictable, and no party can alter it.

7.1 Emission Parameters

Parameter	Value
Maximum Supply	21,000,000 MYT
Initial Block Reward	5 MYT
Halving Interval	2,102,400 blocks (~4 years)
Block Time	60 seconds
Tail Emission	None

7.2 Halving Schedule

The block reward is halved every 2,102,400 blocks — approximately four years at a 60-second block time.

Epoch	Block Height Range	Block Reward
1	0 – 2,102,399	5.000000000 MYT
2	2,102,400 – 4,204,799	2.500000000 MYT
3	4,204,800 – 6,307,199	1.250000000 MYT
4	6,307,200 – 8,409,599	0.625000000 MYT

Internally, all values are represented in atomic units where 1 MYT = 1,000,000,000 (1 billion) atomic units. The initial reward is therefore 5,000,000,000 atomic units. The halving is implemented via integer arithmetic right-shift on this atomic value:

```
halvings = height / HALVING_INTERVAL
reward_atomic = INITIAL_REWARD_ATOMIC >> halvings
```

Because the shift operates on atomic integer units (not floating-point MYT values), the result is always an exact integer with no rounding error. The displayed MYT values (5.0, 2.5, 1.25, 0.625...) are simply the atomic result divided by 1,000,000,000 for human readability. This design is identical in principle to Bitcoin’s satoshi-based emission model.

7.3 No Tail Emission

Once the supply is fully emitted, miner incentivization transitions entirely to transaction fees, preserving the hard supply cap.

8 Privacy & Settlement Security

8.1 Reward Maturity

Coinbase outputs become spendable only after 60 confirmed blocks. This prevents chain reorganization attacks from allowing double-spending of newly mined outputs and ensures settlement finality for miners.

MYT inherits its core privacy stack from the CryptoNote protocol — the same foundation used by Monero. Privacy mechanisms are progressively enforced through the hardfork schedule: RingCT is required from HF6, Bulletproof+ from HF15, and CLSAG ring signatures from HF14. On a mature network (HF16), all mechanisms below are active by consensus and cannot be disabled.

8.2 Ring Signatures

Every transaction input is signed with a ring that includes the real input plus decoy outputs drawn from the blockchain. An observer cannot determine which ring member is the true input. The minimum ring size increases through the hardfork schedule: from 2 at HF2, to 6 at HF7, to 10 at HF8, reaching 15 (with a grace period allowing 10) at HF15. The current consensus-enforced minimum is 16.

8.3 Stealth Addresses

Each transaction generates a unique one-time output address derived from the recipient's public key. An observer scanning the blockchain cannot link multiple transactions to the same recipient without possession of the recipient's private view key. Published addresses are never written to the chain.

8.4 Confidential Transactions

Transaction amounts are cryptographically hidden using Pedersen commitments. The network can verify that inputs equal outputs (no coins created or destroyed) without any party being able to observe the actual values transferred.

8.5 Live Privacy Properties

Privacy Properties — Active on Mainnet

- Sender anonymity: True input concealed within minimum ring of 16 members
- Receiver privacy: One-time stealth addresses — published address never appears on-chain
- Amount confidentiality: All transaction values hidden via Pedersen commitments
- Transaction unlinkability: No cryptographic link between inputs and outputs across transactions

8.6 Practical Limitations of an Early-Stage Network

While the cryptographic mechanisms described above provide strong theoretical privacy guarantees, practical anonymity in a young network depends on the size of the decoy pool. A small transaction history means fewer available decoys, which can reduce the effective anonymity set below the protocol-enforced minimum. As the network grows and transaction history expands, practical privacy properties strengthen. Users operating on mainnet during the early growth phase should be aware of this distinction between protocol-level guarantees and practical anonymity.

9 Ring Size and Anonymity Set

The MYT protocol enforces a minimum ring size at the consensus level. Transactions that do not meet this requirement are rejected by all nodes. Wallet software automatically selects the protocol minimum unless a higher value is specified by the user.

Parameter	Value
Consensus-enforced minimum ring size	16
Wallet default mixin	Automatic (protocol minimum)
Enforcement	Consensus-level rejection of non-compliant transactions

A ring of 16 means every transaction input is signed alongside 15 decoy outputs drawn from the blockchain. As the MYT output set grows with network usage, the quality and diversity of available decoys improves, strengthening practical anonymity over time.

10 Block Size and Scalability

MYT uses a dynamic block weight model. The network adjusts the block weight limit based on recent usage, allowing throughput to scale without hard forks.

Parameter	Value
Max block weight	2 × median block weight
Long-term weight window	100,000 blocks
Full reward zone (primary)	300,000 bytes
Maximum transaction size	1,000,000 bytes

Blocks exceeding median weight receive a penalized reward, creating a market mechanism that naturally calibrates block sizes to actual demand.

11 Network Parameters

11.1 Transaction Fees

MYT implements a dynamic fee model. Fees are calculated from transaction size, median block weight, and the current base block reward — automatically adjusting to network conditions. As halvings reduce the block reward, transaction fees become the primary miner incentive.

11.2 Address Format

MYT uses Base58-encoded addresses. The prefix byte distinguishes network context and address type.

Network	Standard	Integrated	Subaddress
Mainnet	55	56	57
Testnet	155	156	157
Stagenet	255	256	257

Subaddresses generate multiple unlinkable receiving addresses from a single wallet without separate key pairs.

11.3 Protocol Upgrades

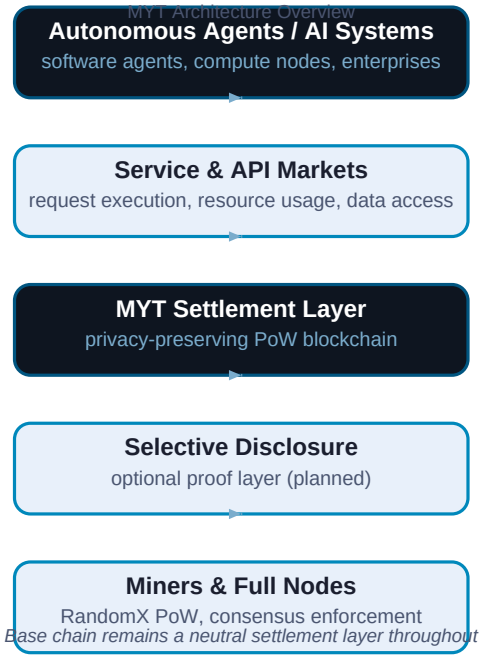
MYT supports versioned protocol upgrades through scheduled hardforks activating at predefined block heights.

Upgrade Mechanism Properties

- Deterministic activation via pre-defined block heights
- Versioned consensus rules with backward-compatible validation
- Optional miner signaling window for upgrade coordination
- No central authority controls upgrade timing or content

12 Machine Settlement Layer

Post-mainnet development introduces infrastructure for autonomous software to perform secure, verifiable, and privacy-preserving financial settlement. The base blockchain protocol remains unchanged. All machine settlement capabilities are optional, higher-layer features. No machine logic is introduced at the consensus layer.



12.1 Why MYT for Machine Settlement?

The question of why autonomous systems should use MYT rather than stablecoins, API credits, or internal balances has a direct answer rooted in four properties that those alternatives cannot simultaneously provide:

The Case for MYT in Machine Economies

– Permissionless access — no account registration, no identity verification, no API key required to transact. Any autonomous agent can participate without prior authorization.

– Privacy-preserving payments — stablecoins and most on-chain systems expose payment flows publicly, leaking operational patterns, infrastructure costs, and business logic of automated systems.

– Non-custodial settlement — unlike API credits or internal balances, MYT cannot be frozen, revoked, or deducted by a third party. Settlement is final when confirmed on-chain.

– Selective disclosure for compliance — when verification is required, agents can generate cryptographic payment proofs without exposing their full transaction history or counterparty relationships.

Together these properties form a settlement stack that is native to autonomous systems: open access, private by default, censorship-resistant, and verifiable on demand.

12.2 Target Use Cases

Primary Use Cases

- AI agents executing autonomous service payments without operator intervention
- Distributed compute networks settling resource usage between nodes
- Automated API economy billing with cryptographic payment verification
- Enterprise machine-to-machine financial interactions requiring audit trails
- Decentralized model inference and data market micropayments

13 Selective Disclosure

All MYT transactions are fully private by default. The following selective disclosure capabilities are planned for future protocol development. They are not currently live on mainnet. Technical specifications including proof system selection (Bulletproofs extensions, zk-SNARK constructions, or hybrid approaches) will be published as development progresses.

Planned Features (Under Development)

- Single-transaction proof: Prove a specific payment occurred without revealing others
- Zero-knowledge audit proof: Verify balance range or transaction set without exposing values
- Counterparty-blind proof: Demonstrate 'I paid X' without identifying the recipient
- Enterprise verification flow: Structured, exportable cryptographic proof artifacts
- API compliance: Settlement verification compatible with automated service contracts

Disclosure is always explicit, opt-in, and controlled by the key holder.

14 Agent Identity Layer

The agent identity layer is a planned off-chain system under active design. The specifications described in this section represent the current architectural direction and are subject to revision as technical design progresses. No agent identity infrastructure is live on mainnet.

14.1 Machine Identifiers

Each agent generates a cryptographic ID from a public key:

```
Machine ID = hash(public_key)
```

This creates a stable, pseudonymous identity without real-world linkage.

14.2 Reputation and Trust

Reputation scores derive from verifiable on-chain settlement history, enabling machine-native trust without institutional vouching.

Planned Architecture (Under Design)

- Cryptographic machine ID: Derived from public key, no real-world linkage
- Signed address binding: Proof that identity controls settlement address
- Settlement reliability score: Derived from verifiable on-chain transaction history
- Trust graph architecture: Machine-to-machine trust without central authority
- Fully off-chain: No identity data on the base blockchain

15 Security Model

15.1 Proof-of-Work Security

An attacker reorganizing the chain must outpace the honest network — requiring majority hashrate and substantial capital. Attack cost scales with total network hashrate.

15.2 ASIC Resistance

RandomX limits specialized hardware advantages, preserving a distributed miner base and improving censorship resistance.

15.3 Double-Spend Prevention

Each input generates a unique key image recorded on-chain. Duplicate key images are rejected, preventing double-spend attempts.

15.4 Sybil Resistance

Block production requires real computational work. Operating additional nodes grants no mining advantage, preventing Sybil-based influence.

15.5 Privacy Attack Resistance

Ring signatures, stealth addresses, and confidential transactions significantly complicate amount-based and graph-based analysis. Increasing ring sizes over protocol versions continuously strengthen the anonymity set.

15.6 Known Early-Stage Risk Factors

Honest security documentation acknowledges the gap between theoretical properties and early-stage operational reality:

Early-Stage Risk Factors

- Lower hash rate than mature PoW networks — 51% attack cost scales with network hashrate
- Smaller decoy pool — practical ring signature anonymity is limited by total transaction history
- Seed node concentration — initial infrastructure operated by core team; expanding over time
- Evolving wallet behavior — edge cases in mixin selection near hardfork transitions
- Limited ecosystem tooling — explorer, wallet, and integration maturity still developing

These factors are characteristic of all early-stage PoW networks, not specific failures of the MYT protocol. They resolve naturally as the network grows.

16 Early Network Considerations

MYT is a live mainnet operating in its early growth phase. The following considerations reflect the honest current state of the network. Acknowledging these realities is not a weakness — it is what separates serious infrastructure projects from speculative ones.

16.1 Hash Rate and Network Security

Early-stage Proof-of-Work networks operate with lower total hash rate than mature networks. A lower hash rate means the cost of a 51% attack is proportionally lower. This is a temporary condition inherent to all new PoW chains. Network security strengthens as mining participation grows. Users and services should apply appropriate confirmation depth requirements during the network's early phase.

16.2 Anonymity Set Size

The practical strength of ring signature privacy depends on the size of the available decoy pool. With fewer total transactions on-chain, the effective anonymity set is smaller than it will be once the network matures. The protocol enforces a minimum ring size of 16, but the value of that ring is directly correlated with the diversity of the underlying output set. Privacy improves as transaction volume grows.

16.3 Tooling and Infrastructure Maturity

Wallet software, block explorers, and third-party integrations are functional but continue to evolve. Edge cases in wallet behavior — particularly around mixin selection during hardfork transitions — may exist and are actively addressed during development.

16.4 Exchange and Ecosystem Integration

As a newly launched network, MYT does not yet have broad exchange listings or extensive third-party service integration. Ecosystem development is an ongoing process that follows network stability.

16.5 Early Infrastructure Concentration

Initial seed nodes and public infrastructure are operated by the core development team. While the protocol itself is permissionless and decentralized, early infrastructure concentration is a practical reality of network bootstrapping. Expanding the set of independent node operators is a priority for long-term decentralization.

17 Development Roadmap

Phase 1 — Local Testnet (Completed)

Core chain logic validated: deterministic block production, wallet-daemon communication, mining, stable RPC, and transaction processing confirmed.

Phase 2 — Public Testnet (Completed)

MYT operated in a live network environment: public seed nodes, external wallet connectivity, multi-node sync, block explorer, reproducible builds, and network health metrics deployed. Network stability confirmed.

Phase 3 — Mainnet (Live)

Mainnet is live. All consensus parameters finalized and deployed. Deterministic release builds available for Linux and Windows. Public infrastructure stable and operational.

Phase 4 — Machine Settlement Layer (Active Development)

Layered capabilities being built on top of the base protocol: selective disclosure proofs, cryptographic machine identity, and agent reputation infrastructure. No consensus centralization. The base chain remains a neutral settlement layer throughout.

18 Conclusion

MYT is financial infrastructure for the next phase of the digital economy — one in which autonomous systems transact programmatically, enterprises require verifiable settlement without surveillance, and individuals demand genuine financial privacy.

With CryptoNote-derived privacy, RandomX Proof-of-Work, and Bitcoin-style monetary policy, MYT provides a technically sound and economically predictable foundation. Future extensions — selective disclosure, machine identity, settlement verification — build on this foundation without compromising its core neutrality.

MYT does not optimize for short-term speculation. It is built to be infrastructure — reliable, deterministic, and still useful decades from now.

Appendix A — Core Network Parameters

Parameter	Value
Consensus Mechanism	Proof-of-Work
Mining Algorithm	CryptoNight (launch) → RandomX (HF12, block 28,895)
Block Time	60 seconds
Maximum Supply	21,000,000 MYT
Initial Block Reward	5 MYT (5,000,000,000 atomic units)
Atomic Unit	0.000000001 MYT (10^-9, 1 billionth)
Halving Interval	2,102,400 blocks (≈4 years)
Coinbase Unlock Window	60 blocks
Minimum Ring Size	16 (consensus enforced)
Address Prefix — Mainnet Standard	55
Address Prefix — Mainnet Integrated	56
Address Prefix — Mainnet Subaddress	57
P2P Port	39080
RPC Port	39081
ZMQ Port	39082
Difficulty Window	720 blocks
Difficulty Lag	15 blocks
Difficulty Cut	60 (outlier trimming)
Full Reward Zone	300,000 bytes
Max Transaction Size	1,000,000 bytes
Tail Emission	None

Appendix B — Design Constraints

The following constraints are enforced at the protocol level and will not be altered through future upgrades:

- No AI in consensus: Autonomous agents may use MYT but cannot control validation
- No identity enforcement: The base chain enforces no identity requirements
- No central upgrade authority: Protocol changes require broad adoption
- Fixed supply: The 21,000,000 MYT cap is a consensus rule
- Privacy by default: Transaction privacy cannot be disabled at protocol level

Appendix C — Network Resources & Verification

The following resources allow independent verification of the MYT protocol implementation, network state, and infrastructure.

Resource	Details
Source Code	github.com/myt-core/MYT
Mining Algorithm	RandomX (CPU-optimized, ASIC-resistant)
Build Reproducibility	Deterministic builds — Linux & Windows

Independent Verification

- Source code is publicly available at github.com/myt-core/MYT
- Any node operator can independently verify consensus rules by running a full node
- Block explorers and additional infrastructure details published on the project repository
- Deterministic build instructions included in repository documentation

Disclaimer: This document is a technical overview and development roadmap. It does not constitute an offer of securities, financial advice, or investment recommendation. MYT is live software; parameters described herein reflect the deployed mainnet configuration. Planned features (Sections 11–13) are under active development and subject to revision.