📜 Veritas: Protocol of Transparent Trust

Whitepaper — Draft v1.0

---

1. Introduction

In the world of cryptocurrencies, transparency, user protection, and modern UX are often lacking. Veritas is a new digital currency that combines quantum-resistant cryptography, built-in two-factor authentication (2FA), single-use addresses, and a transparent architecture with a reserve mechanism. Its goal is to build an infrastructure of trust — not just another token.

---

2. Philosophy and Values

Veritas is built on three core principles:

- **Transparency**: every transaction has an audit trail
- **Control**: users own their keys and confirm actions via 2FA
- **Security**: quantum-resistant cryptography, cold storage, and ephemeral addresses

“This is not just a currency. It’s a protocol of trust. Every key is a choice. Every transaction is an act of transparency.”

---

3. Protocol Architecture

- Single-use addresses with TTL
- 2FA via mobile devices or USB keys
- Local authorization agent
- Falcon/Dilithium transaction signatures
- Open blockchain + reserve server for logs

---

4. Cryptography and Security

- **Signature**: Falcon or Dilithium (NIST PQC finalists)
- **Hashing**: SHA3 or Blake3
- **Address**: derived from public key + metadata
- **Cold storage**: hardware wallet support

---

5. 2FA and UX

- Biometrics, OTP, USB keys
- Local agent verifies 2FA before broadcasting transaction
- Mobile app with intuitive interface
- QR/NFC integration for payments

---

6. Single-Use Addresses

- Generated on demand: amount, merchant ID, TTL
- Used once, then expires
- Can be embedded in QR code or NFC token
- Reduces address reuse risks

---

7. Transparency and Reserve

- Open blockchain with audit trail
- Reserve server:
  - stores authorization logs
  - has no access to private keys
  - used for dispute resolution and recovery

---

8. Stability Model

- Algorithmic reserve or multi-asset backing
- Transparent emission model
- Fixed transaction fees
- Optional peg to asset basket

---

9. Comparison with BTC, ETH, Stablecoins

Feature	BTC	ETH	Stablecoins	Veritas
2FA	✗	✗	✗	✓
Single-use addresses	✗	✗	✗	✓
Quantum resistance	✗	✗	✗	✓
UX	□	□	✓	✓✓
Reserve transparency	✗	✗	□	✓

---

10. Roadmap and MVP

- **Q1**: MVP — address generation, 2FA, signing
- **Q2**: mobile app, QR/NFC integration
- **Q3**: payment system integration
- **Q4**: mainnet launch, audit, public release

---

11. Legal and Copyright

- Timestamp via OpenTimestamps or email
- Digital signature via DocuSign or Artlogo
- Publication on GitHub or IPFS
- License: Creative Commons or MIT

---

12. Conclusion

Veritas sets a new standard for transparency, security, and user control. It’s not just a currency — it’s a trust infrastructure capable of competing with BTC, ETH, and stablecoins by offering a unique blend of UX, cryptographic integrity, and philosophical clarity.
