



EVERVEST

(WHITE PAPER)

1. INTRODUCTION

UTXO vs Account Models?

Traditional Ledger vs EVST Ledger?

The EverVest network combines the best aspects of modern decentralized ledger technologies. Today's decentralized ledgers are divided into two groups. One group supports the **UTXO model**, which is scalable, privacy-friendly, and supports simple payments. The other group uses an **account-based model**, which supports smart contracts and forms the basis for decentralized finance (DeFi) and other decentralized applications.

In ledgers like Bitcoin, the fundamental value unit is called an **unspent transaction output (UTXO)**. Each UTXO has a value and an owner. In the real world, if you use a \$10 bill to buy a \$5 coffee, you hand the cashier the bill and receive \$5 in change along with your coffee. Similarly, when you buy a \$5 coffee with a \$10 UTXO, you create a transaction with one input (the \$10 UTXO) and two outputs (the \$5 UTXO sent to the cashier and a \$5 change UTXO sent to your own address).

In ledgers like Ethereum, each unit of value is associated with an account, and that account has a balance. To buy a \$5 coffee, you simply transfer \$5 from your account to the cashier's account.

Each model has its own advantages. The UTXO model is potentially more scalable because transactions can be independently verified without needing to track account balances. Additionally, the UTXO model provides enhanced privacy, as users can create new output addresses for each transaction, whereas the account model directly links balances to the user's account.

However, the account model also has appealing features. It facilitates the use of **smart contracts** that can control and manage assets. Smart contracts form the foundation of decentralized finance (DeFi) and other advanced decentralized applications (dApps).

EverVest Network: Combining the Best Features

The EverVest network supports both UTXO and account models. EverVest's UTXO model supports fast and scalable payments, while its Ethereum Virtual Machine (EVM)-compatible account-based subsystem supports standard smart contracts. A library that combines these two worlds enables developers to take advantage of the benefits of both models.

Most decentralized ledgers are structured as **linear chains of blocks (blockchains)**. Each block contains transactions in a linear order (which could be either UTXO or account-based). This linear structure is intuitively logical, as the order in which transactions are executed may matter, and all parties must agree on that order. However, linear blockchains can face scalability issues because each node must process all transactions, which can slow down transaction times and increase transaction fees.

Moreover, many transactions are independent, meaning they do not need to be executed in a specific order. To avoid the costs of enforcing a strict order between transactions, researchers have developed various algorithms for **partial ordering** of transactions. This method allows unrelated transactions to be validated in parallel and added to the ledger. The resulting ledger is not a linear blockchain, but rather a **directed acyclic graph (EVST)** structure.

EverVest's EVST Structure

EverVest supports an EVST-based ledger using a version of the **Phantom GhostEVST protocol**. Simply put, a block is added to the ledger once it becomes sufficiently connected to previous blocks, and its permanence is highly likely to be guaranteed. As the EVST grows, the **GhostEVST algorithm** ensures that a universally accepted linear ordering of blocks eventually emerges.

EverVest is fully compatible with the Ethereum Virtual Machine (EVM), enabling seamless integration and deployment of Ethereum-based smart contracts. This compatibility allows developers familiar with **Solidity** and other Ethereum-compatible programming languages to easily build and deploy decentralized applications (dApps) on the EverVest network. Developers can port existing Ethereum dApps and tokens to EverVest with minimal changes.

EverVest also supports popular Ethereum development tools like **Truffle**, **Remix**, **MetaMask**, and **Hardhat**, making the development and deployment process easier. EverVest supports Ethereum token standards such as **ERC-20** (fungible tokens) and **ERC-721** (non-fungible tokens), facilitating token issuance and smart contract functionality.

UTXO-EVM Bridge

EverVest's native currency, **EVST**, can be transferred between the UTXO domain and the EVM domain, and vice versa. A token can only exist in one domain at a time, and the conversion rate between the two is 1:1.

To transfer tokens from the EVM domain to the UTXO domain, the following steps are followed:

1. The user requests to burn their tokens on the EVM side.
2. The EVM side initiates the burn process and notifies the synchronization layer that the tokens have been burned.
3. The synchronization layer verifies that the burn operation has been finalized on the chain, then informs the asset management layer.
4. After the necessary checks, the asset management layer issues the same amount of tokens on the UTXO side.
5. If all steps are completed successfully, the UTXO side assigns the newly minted tokens to the user's account and notifies the user that the transfer is complete.
6. The synchronization layer confirms to the EVM side that the UTXO tokens have been issued, and the EVM side then informs the user that the transfer is successful.
7. If the synchronization layer waits too long to confirm the burn operation, it notifies the EVM side that the transfer has failed, and the EVM side informs the user of the failure.

Traditional individual retirement systems involve high commission rates, liquidity restrictions, and manipulation risks due to their centralized structures. The blockchain-based decentralized individual retirement system **EverVest** aims to provide participants with a **100% transparent, secure, and profitable** retirement plan. EverVest enhances **financial independence** by offering investors flexibility in funding through professional advisors or individual selections.

EverVest Transaction Lifecycle

Transaction Process Flow

Consensus

The heart of EverVest's consensus mechanism is a **Proof-of-Work (PoW)** algorithm. Like most PoW chains, a miner assembles a block by combining transactions with a block header. One field in the block header is called the **nonce**. The miner's task is to find a nonce such that the resulting hash of the entire block produces a value consistent with the current difficulty level of the chain.

In conventional blockchains, only one miner at a time can solve the hash puzzle to produce a new block. EverVest, in contrast, allows for **concurrent block production**, where miners operating in parallel can both produce blocks. For more details on how this works, please refer to the **GHOSTEVST protocol** section.

Blocks are considered final once they have been referenced by enough later blocks in the **EVST**. Even though multiple blocks can be produced at the same time, the network eventually reaches consensus on the order and validity of transactions. The miner consensus protocol is broken into several layers:

1. Peer-to-Peer (P2P) Network:

EverVest uses a **peer-to-peer (P2P) network** to disseminate transactions and blocks across the network. The P2P network performs basic validity checks on transactions and blocks as they are transmitted.

- **TCP/IP** is used for reliable, connection-oriented communication between nodes.
- **UDP** is used for efficient, connectionless discovery of new peers.

2. Transaction Fees:

EverVest supports both **UTXO** and **EVM** models for transaction fees.

- For **UTXO transactions**, a fee is attached to each transaction, similar to Bitcoin. The first miner to mine a block containing the transaction is awarded that fee. Fees function as an auction, where transactions bid to be included in a block. Users should attach higher fees to higher-priority transactions. When the network is busy, fees will rise.
- For **EVM transactions**, a **gas fee** system similar to Ethereum is used. A user pays a certain amount of gas for each computational step a smart contract executes.
- Initially, there will be a **\$0.01 per transaction** fee, with the distribution as follows:
 - **50%** goes to the miner,
 - The remaining **50%** is split between the network and the originating **dApp**.

3. PoW Verification Engine:

- The **block reception layer** accepts blocks from the peer-to-peer network, performs preliminary checks, and updates the EVST topology.
 - The **PoW verification engine** tracks the current difficulty level, applies further verification, and searches for and verifies the miner's solution to the cryptographic puzzle.
 - The **SPECTRE protocol layer** establishes a **partial order** on the blocks in the EVST.
 - The **PHANTOM protocol layer** extends this partial order into a **stable and secure total order**.
 - The **consensus formulation layer** determines the new network difficulty for subsequent PoW consensus and updates the chain state (UTXOs, EVM account balances, and smart contract variables).
-

Security

Security is a cornerstone of EverVest. The system employs the following advanced cryptographic techniques to secure transactions, validate blocks, and protect against malicious activities:

- **Public/Private Key Encryption:** EverVest uses asymmetric encryption for transaction signing and validation. Each participant has a **private key** for signing transactions and a **public key** for others to verify those signatures.
- **Hashing:** Blocks and transactions are hashed using a secure cryptographic algorithm (e.g., **SHA-256**) to ensure data integrity and prevent tampering.
- **Proof of Work (PoW):** EverVest employs a **PoW-based consensus mechanism**. Miners solve cryptographic puzzles to validate new blocks and add them to the EVST, ensuring the network is resistant to attacks such as **double-spending** or **51% attacks**.
- **DDoS Protection:** Mechanisms such as **rate-limiting** and **anti-spam filtering** are built into the network layer to prevent **Distributed Denial-of-Service (DDoS)** attacks.
- **Sybil Attack Resistance:** By requiring proof of computational work, EverVest resists **Sybil attacks**, where an attacker tries to flood the network with fake traffic.

EverVest's security is built on the **GHOSTEVST protocol**, which is used to generate and order blocks. This protocol allows miners to produce blocks in parallel and ensures that the network can distinguish between blocks mined by honest miners and those possibly mined by dishonest ones.

- A block that is **strongly connected to previously verified honest blocks** is highly likely to be honest.
 - A block that is only **weakly connected to honest blocks** is likely to be dishonest.
 - The **PHANTOM protocol** converts the **partial order** of blocks into a **total order** that all honest observers will agree on, ensuring the chain's stability.
-

UTXO-EVM Bridge

EverVest's native coin, **EVST**, can be transferred between **UTXO** and **EVM domains**. However, a coin cannot exist in both domains at the same time. Coins are **converted in a 1:1 ratio**.

The transfer process from EVM to UTXO is as follows:

1. The user requests that coins in the EVM domain be burned.
2. The EVM system burns the coins and notifies the synchronization layer that the process is complete.
3. The synchronization layer confirms that the transaction is finalized and informs the asset management layer.
4. The necessary checks are performed, and an equivalent number of coins are created in the UTXO domain.
5. The UTXO system assigns the new coins to the user and notifies them that the transfer is complete.
6. If the synchronization process is delayed, the EVM side will notify the user that the transaction has failed.

Transfers from UTXO to EVM follow the same process and are symmetric.

EverVest is fully **compatible with the Ethereum Virtual Machine (EVM)**, supporting decentralized finance (DeFi) and smart contracts. Ethereum-based applications (**dApps**) and tokens can be transferred to **EverVest** with minimal changes. Popular standards like **ERC-20** (fungible tokens) and **ERC-721** (NFTs) are also supported.

Through this, EverVest aims to offer a **fast, scalable, and secure blockchain network** that is fully compatible with the **Ethereum ecosystem**. 

1.1 History and Current Status of EverVest

- The development of the EverVest project began in **2021**.
 - In **2022**, the system became fully operational and was made available to our users.
 - **Our decentralized retirement system project is under development and will be launched soon.**
-

2. EVERVEST SYSTEM MECHANISM

- **Maturity Options:** Minimum **1 year**, maximum **4 years**.
 - **Investment Amounts:** Minimum **\$1,000** - Maximum **\$100,000**.
 - **Monthly Return:** **7%** of the investment amount will be reflected in the system as cash and can be used for funding.
 - **Monthly Investment Option:** Users can increase their investments monthly and make additional funding.
 - **Withdrawal Rules:** **Funds cannot be withdrawn before maturity.**
 - **Funding:** Can be done individually or through professional investment advisors.
 - **Return Distribution:** Investors can manage their portfolios individually or professionally and receive returns transparently **through smart contracts**.
-

2.1 EverVest Investor Return Simulation

Investor earnings vary based on the committed maturity period:

Year	Investment Amount (\$)	Amount Transferred to Funding Account (\$)	Usable Return (\$)
------	------------------------	--------------------------------------------	--------------------

1	2,000	140	2,140
2	2,000	280	2,280
3	2,000	420	2,420
4	2,000	560	2,560

3. BLOCKCHAIN INTEGRATION AND DECENTRALIZATION

- **Smart Contracts:** All fund movements will be carried out **transparently** and **auditable** through smart contracts.
 - **DAO (Decentralized Autonomous Organization):** A community-driven governance system may be implemented.
 - **Security:** Funds will be secured by being stored in decentralized wallets and on smart contracts.
 - **Transparency and Auditability:** Users can monitor the transaction history on the blockchain to verify the system's operation.
-

4. EVERVEST TOKEN ECONOMY (TOKENOMICS)

- **1st Presale:** 10% of tokens will be offered at **\$0.002** per unit.
 - **2nd Presale:** 15% of tokens will be offered at **\$0.005** per unit.
 - **3rd Presale:** 25% of tokens will be offered at **\$0.02** per unit.
 - **Airdrop Process:** Will be conducted in **28-day cycles**.
 - **Exchange Listings:** Planned for **SEPTEMBER 2025** on Binance, Gate.io, PancakeSwap, and similar exchanges.
 - **Staking Benefits:** EverVest token holders can earn **passive income through staking**.
 - **Exclusive Early Investment Opportunities:** Early investors in EverVest will benefit from **bonus tokens and special advantages**.
-

5. EVERVEST REVENUE MODEL AND COMMISSIONS

- **Commission Deductions:** **90% of collected commission fees will be returned to users.** To sustain the system, **10% will be held on the blockchain**.
 - **Professional Investment Advisors:** Users can entrust their assets to professionals based on designated fund strategies.
 - **Sustainability:** The platform will offer a **dynamic revenue-sharing model** to ensure users earn long-term income.
-

6. EVERVEST ROADMAP

- **2023:** Concept development phase of the EverVest project.
 - **2024:** Completion of blockchain infrastructure and initiation of testing phases.
 - **Q2 2025:** Token supply planning, expansion of the investor base, and announcement of new features.
 - **Q4 2025:** Listing EverVest token on major exchanges and executing large-scale marketing campaigns.
 - **Q6 2025:** Inclusion of initial users in the platform, initiation of first investment and funding processes.
 - **2026 and beyond:** Integration of DAO governance system, expansion into global markets, and continuous ecosystem development.
-

7. EVERVEST TEAM AND PARTNERSHIPS

The EverVest project team consists of experts in **finance, blockchain, and software**. Additionally, strategic partnerships are targeted to support ecosystem development. With a **strong investor and advisory team**, the project aims to establish a **sustainable financial ecosystem**.

 Our decentralized retirement system project is under development and will be launched soon.