Bullish

NEWS RELEASE

Bullish Custody: Navigating the future of digital asset security

2024-04-26

TLDR; This blog introduces Bullish exchange's advanced custody solutions[1], emphasizing the role of the Taurus Blockchain, Smart Contracts, Oracles, Multi-Party Computation (MPC), and Trusted Execution Environments (TEEs) in asset protection. We detail our use of Warm and Cold Wallets for asset management and discuss integrating Artificial Intelligence (AI) to enhance development and operations. The upcoming series will further dive into these technologies, starting with the Taurus Blockchain's architecture.

By Mothusi Majinda, Chief Technology Officer, Alun Davies, Mohammad Nauman, Santhosh Kumaraswamy, Directors of Engineering

[1]Custody solutions provided by members of the Bullish Group (1) may differ in particular jurisdictions to meet regulatory and customer requirements and expectations; and (2) will continue to evolve over time, so the information in this blogpost may become outdated. Please reach out to **support@bullish.com** if you would like to understand the approach currently used to protect customer assets in your jurisdiction.

In the rapidly evolving digital finance landscape, Bullish focuses on advancing the security and reliability of digital asset custody. Our focus is to make cryptocurrency management as commonplace and reliable as traditional banking.

Central to this effort is the Bullish User Interface (UI) portal, serving as the gateway for customers to manage their digital assets securely. Integral to the custody process is the Bullish Custody API Gateway, acting as a conduit for all transactions. In coordination with our network of modular oracles, the gateway initiates a series of tasks and compliance checks. These oracles, specifically designed for distinct functions: for instance, the Fiat Oracle facilitates communication with banks, the AML Oracle integrates with AML providers for compliance checks, the Custody

Oracle ensures seamless integration with third-party custody solutions or Bullish's own custody services, and the Exchange Gateway Oracle integrates directly with the Trading Engine. Each oracle is tailored for specific tasks, enhancing the system's flexibility and adaptability. These oracles play crucial roles in validation and execution, ensuring transactions meet stringent security standards and integrate seamlessly with Taurus for further processing.

Taurus, a private and permissioned blockchain, is deeply integrated into the entire transaction lifecycle, not just as a ledger for compliance audit trails. It begins with the transaction's inception, ensuring each step adheres to our stringent security and business rules. Leveraging a single block producer model for high availability, Taurus guarantees transaction order and provides advanced multi-signature security, crucial for preventing insider attacks and ensuring transactions originate from authorized entities.

Transactions are verified and recorded by Taurus, providing complete auditability and idempotency for actions like deposits and withdrawals, and administering new digital instrument listings. The blockchain architecture is designed for resilience, with nodes distributed across multiple availability zones and regions, dramatically reducing the risk of failures that could impact our customers. Taurus provides a stable and scalable foundation that allows Bullish Custody to operate with the precision and reliability required for a regulated exchange in the digital asset space.

The Bullish Trading Engine ensures seamless trade execution, with a design that balances rapid order processing while engaging the Taurus blockchain for crucial custody operations. Instead of interacting with the blockchain in real-time for each trade, Taurus is integral during key custody events like deposits and withdrawals. Here's how it works: as part of the first deposit request, Taurus allocates a unique address to the customer, which is used to receive assets and record the transaction. When these assets are deposited to the provided address on the public blockchain, Taurus, along with Bullish Custody or a third-party custodian, indexes the transaction and records it, ensuring that once confirmed, the customer's balance is accurately reflected within our trading engine. Withdrawal requests undergo rigorous checks, including AML compliance and balance verification, before being executed through Bullish or third-party custodians, ensuring security and integrity throughout. This strategic approach prioritizes transaction integrity and custody security without compromising the system's responsiveness.

Bullish employs a multi-custodian strategy, combining our internal custody solution with third-party custodial services. This approach reflects our philosophy of offering a secure, reliable, and resilient custody solution that customers can depend on. Looking closer at our Bullish Custody, we find a system of precision-engineered modules working in concert to manage transactions across various Layer 1 blockchains. The Transaction Builder carefully prepares raw transactions, which are then authorized and managed by the Transaction Manager. Alongside, our Layer 1 indexers tirelessly track public blockchain activities, ensuring that every transaction is recorded accurately

in Taurus, thereby maintaining the integrity of asset management within Bullish.

In addition to our robust custody solutions, the management and security of customer's assets are further enhanced by the strategic use of Bullish exchange wallets. Deposits from our customers are initially directed to Warm Wallets, ensuring that all incoming assets are processed securely and efficiently. For withdrawals, we utilize Hot Wallets, designed to facilitate swift and secure transactions. Importantly, the majority of customer's assets are stored in Cold Wallets, providing an additional layer of security by keeping these funds offline in cold storage. Our dedicated Custody Operations team continuously monitors transactions related to deposits or withdrawals, regularly reviewing and rebalancing assets between wallets. This meticulous management ensures there is always sufficient liquidity for smooth operations, while also prioritizing the safeguarding of assets by keeping the bulk of funds securely offline.

Our security measures include an advanced Multi-Party Computation (MPC) solution, which is highly scalable and secure, and has been thoroughly examined by the independent auditor, **Verichains**. Our MPC technology is recognized as highly secure, exemplifying our continuous effort to protect customer's assets. All of our custody components managing the sensitive and confidential workload, including custody oracles, gateways, and MPC nodes, are running in a Trusted Execution Environment (TEE) provided through secure and hardened infrastructure backed with Trusted Platform Modules (TPMs).

In conjunction with these security measures, Bullish exchange is **leveraging AI** to further refine our development and operational processes. Beyond traditional anomaly detection through Machine Learning, we're implementing Generative AI for test automation, enhancing our capacity for writing unit and integration tests. This approach not only shifts quality assurance from right to left but also paves the way for AI's deeper integration into our development workflow, promising improved efficiency and a better developer experience.

As we continue our journey, the integration of blockchain and AI technologies underscores our dedication to providing secure, innovative services. The exploration into our custody solutions is just the beginning. Upcoming segments will delve into the architectural nuances of the Taurus Blockchain, among other core technologies. Stay with us as we unpack how each technological pillar, from Smart Contracts to Secure Infrastructure, fortifies Bullish's cutting-edge custody solutions.

Feeling inspired by the cutting-edge work we're doing at Bullish? We're always on the lookout for talented individuals to join our team. **Explore our open roles** and be Bullish on your career. Want to stay up to date with the latest news from across Bullish? Follow us on **LinkedIn** and **X**.

ARE YOU BULLISH?

Take charge and be Bullish on your career by helping us build the best digital asset trading platform for institutions.

Work at Bullish