Bullish

NEWS RELEASE

Bullish Custody: Foundation of trust – exploring the Taurus blockchain’s architectural evolution

2024-06-18

TLDR; This post explores the advanced architecture of the recently open-sourced Taurus blockchain, essential to the high-performance and secure operations at Bullish exchange. It underscores the role of Taurus as a critical foundation for trust within our Bullish Custody Platform, reflecting our commitment to transparency and innovation. Through its development, significant enhancements have been made to the EOSIO framework, establishing a solid foundation for a high-performance exchange. These advancements provide valuable assets to the broader community, enabling the application of the Taurus blockchain across various use cases.

By Kevin Xia, Farhad Shahabi, Senior Engineers, Eric Ma, Santhosh Kumaraswamy, Mohammad Nauman, Directors of Engineering

In our ongoing series detailing the sophisticated custody solutions[1] at Bullish, this entry focuses on the Taurus blockchain, a cornerstone of security and reliability in digital asset management. For those who have not read our introductory blog, "**Bullish Custody: Navigating the future of digital asset security**," we recommend starting there to gain a comprehensive overview of the series' context. Recently open-sourced, the **Taurus blockchain**, built on the refined and tailored EOSIO framework specifically for enterprise-grade performance, now invites the global developer community to explore its capabilities and contribute to its continuous evolution.

This blog delves deep into the architectural nuances and strategic importance of Taurus, elucidating why it's more than just a blockchain—it's a foundation of trust in our Bullish Custody Platform. The decision to open source Taurus underscores our commitment to transparency and enables further applications and innovation in the community. Through its development journey, Bullish has garnered significant insights and made extensive refinements to bolster EOSIO's capabilities, providing a robust foundation for a high-performance exchange. These

learnings and the battle-tested software are invaluable assets to the wider community, enabling further applications using the Taurus blockchain software.

1. Why use a private blockchain for Bullish

Adopting a private blockchain at Bullish is strategic, driven by the need for enhanced security, customized control, and optimized performance that are critical in managing digital assets securely and efficiently. Private blockchains provide the flexibility necessary for adapting to the complex regulatory and operational requirements of the financial industry.

1.1 Ensuring security with cryptographic proofs

Taurus secures every blockchain interaction through cryptographic signatures, requiring dual-key authorization for transactions and block signing. This ensures all operations are traceable and protected against tampering, establishing a secure infrastructure critical for asset protection. Each transaction requires authorization via keys that are rigorously managed within Bullish's secure infrastructure, ensuring cryptographically provable states. The dual-key mechanism (one for initiating transactions and another for block signing by the block producer) is designed to ensure that every operation on the blockchain is traceable and tamper-proof. Keys within Bullish are protected by multiple layers of security, providing robust defense against unauthorized access and potential security breaches.

1.2 Ensuring predictable outcomes with deterministic transaction execution

The smart contracts on Taurus execute transactions with deterministic outcomes, generating consistently predictable and reliable results. This consistency is crucial for maintaining the integrity of core business processes and supports repeatable validation processes essential for auditing and regulatory compliance. Such deterministic processing is crucial for maintaining seamless continuity and integrity across Bullish's financial operations, enhancing both security and operational predictability. This reliability in transaction execution allows Bullish to uphold stringent standards in transaction processing, crucial for customer trust and regulatory approval.

1.3 Strengthening system integrity with cross-validation and safety guarantees

Each node within the Taurus blockchain is designed to operate under a zero-trust model, rigorously validating every transaction, block, and signature independently. This extensive cross-validation forms a comprehensive safety net, ensuring all operations adhere to the highest security standards. The producer-validation-trust loop integral to Taurus ensures that each component in the transaction chain is verified without any presumption of trust, enhancing security against insider threats and systemic errors. This robust validation framework not only secures transactions but also fortifies the overall system against vulnerabilities, making Taurus a reliable platform for high-stakes financial operations.

1.4 Enhancing accountability with full traceability

In Taurus, every transaction is immutably and permanently recorded, allowing for full traceability from inception to execution. This capability not only supports regulatory compliance and operational auditing but also enhances overall operational transparency, enabling Bullish and its regulators to meticulously trace operations for integrity and accuracy. Full traceability is crucial in the digital asset space, where transparency can significantly influence trust and compliance, ensuring that all stakeholders have access to a clear and unalterable history of transactions.

1.5 Ensuring data integrity with immutable history

Once recorded on the Taurus blockchain, transactions cannot be altered or deleted, ensuring an immutable historical record of all operations. This immutability safeguards the history of asset transactions against tampering, enhancing the security and reliability of the custody solution. Internal and external documentation, such as logs and video recordings that track blockchain hashes, provide additional layers of historical evidence, further securing the integrity of recorded data. This permanent record is a foundational aspect of Bullish's commitment to providing a secure and trustworthy platform.

1.6 Prioritizing customer privacy with advanced data protection

While facilitating transaction validation and system audits, Taurus is meticulously engineered to safeguard user privacy. Advanced cryptographic techniques and access controls protect customer data while complying with stringent regulatory standards. The virtualization of records on Taurus ensures that they do not reveal sensitive customer information, yet remain sufficient for business logic validation. This dedication to privacy helps Bullish maintain customer trust and meet global compliance standards, which are particularly stringent in the financial industry.

1.7 Delivering high performance and enterprise-level features

Engineered to support Bullish's round-the-clock trading operations, Taurus leverages enhancements from the EOSIO codebase to deliver exceptional performance, low latency, and scalability. These capabilities allow the blockchain to handle high transaction volumes typical of major financial markets without sacrificing speed or reliability. This performance is bolstered by advanced features such as producer high availability, disaster recovery protocols, and the ability to scale dynamically in response to varying loads. Additionally, the Query Service provides a REST interface that allows for efficient querying of the Taurus blockchain. This service enables developers and system operators to perform sophisticated queries, troubleshoot, and debug, enhancing accessibility and operational efficiency. Enhancements also include support for the Protobuf data type, which simplifies Smart Contracts and Oracles interactions, further streamlining blockchain operations. These features allow Taurus to meet the demanding requirements of enterprise-level blockchain applications, providing a stable and robust platform for Bullish's operations.

2. Evolution of Taurus architecture at Bullish

The architectural evolution of the Taurus blockchain at Bullish is driven by the ever-evolving needs of the digital asset market and our operational requirements. Each generation of architecture has been a step forward in enhancing the security, efficiency, and scalability of the platform, directly responding to the increasing complexity and demands of the industry.

2.1 First generation: On-chain architecture

The initial architecture of Taurus was wholly on-chain, with every component of the trading engine and custody solutions implemented as smart contracts on the blockchain. This design leveraged the high-performance capabilities of the EOSIO software, establishing a robust foundation for secure transaction processing and data integrity. However, as transaction volumes grew, this first generation faced scalability and latency limitations, necessitating an architectural evolution to better meet the dynamic demands of Bullish's expanding market presence.

2.2 Second generation: Hybrid architecture

In response to these scalability challenges and to enhance performance, Bullish evolved into a hybrid architecture. This new phase involved a partial migration of certain operations off-chain while maintaining critical blockchain functions for transaction validation and record integrity. The hybrid model significantly reduced latency and improved transaction throughput, enabling Bullish to manage increased trading volumes without compromising the security and reliability inherent in the blockchain.

2.3 Third generation: Enhanced customer-focused architecture

The third generation of Bullish’s architecture around Taurus focuses on operational simplicity and efficiency. It minimizes system redundancies and strengthens core components to optimize maintenance and performance. This refined architecture boosts Bullish’s ability to handle substantial workloads, particularly for the Bullish Custody Platform, leveraging foundational blockchain features such as cryptographic provability, deterministic behavior, full traceability, and rigorous control mechanisms. These elements ensure the integrity and security of transactions, providing a reliable platform for asset management. The design emphasizes safeguarding customer assets with enhanced security measures and improved system responsiveness, and includes technical enhancements that contribute to system scalability and reliability. Improved smart contract functionalities and better integration with external systems support real-time processing capabilities and more efficient user interactions.

This evolution not only highlights Bullish's commitment to adaptation and growth but also underscores how past enhancements have solidified the foundation of the Taurus blockchain, making it a dependable and scalable platform ready to meet future demands.

3. Architecture of the Bullish Taurus blockchain

As an enterprise-level application platform, Taurus is designed to meet the demanding needs of modern

enterprises. It offers a robust suite of functionalities and interfaces essential for efficient blockchain integration. This architecture not only supports current operational demands but is also engineered to adapt to future technological shifts, supporting long-term sustainability and scalability.

3.1 Taurus functionalities

Taurus plays a multifaceted role within the blockchain ecosystem, primarily serving oracles that act as the intermediaries between the blockchain and external applications. Key functionalities include:

- Transaction processing: Taurus processes signed transactions that trigger actions within smart contracts, crucial for maintaining the blockchain's state. This includes deploying or updating smart contracts, creating accounts, and managing keys, effectively serving as the gateway for all data and requests entering the blockchain.
- Query handling: Taurus supports queries executed through dedicated smart contracts, enabling efficient data retrieval. This is vital for applications that interact dynamically with the blockchain, allowing them to access needed data for further processing.
- Event streaming: Taurus captures and streams real-time events generated during smart contract execution. This functionality enhances the system's responsiveness, allowing oracles to receive immediate updates essential for operations requiring quick data reflection.

The business logic behind those functionalities are primarily through smart contracts, allowing for significant customization to meet specific enterprise needs.

3.2 Taurus interfaces

Taurus provides robust interfacing capabilities designed for seamless integration with enterprise applications, maintaining functionality even during failover scenarios:

- Message queues: Taurus utilizes RabbitMQ within the Advanced Message Queuing Protocol (AMQP) framework to manage the flow of transactions and events efficiently. This queuing system is crucial for handling inputs from transactions pushed by oracles and outputs from events generated within the Taurus blockchain. Its robust architecture allows each component within the system to operate independently, ensuring high availability. If a node fails, the system can seamlessly fail over to a standby process without impacting ongoing operations, preserving operational continuity even during periods of heavy load.

  RabbitMQ serves as a buffer during these peak times, preventing the system from being overwhelmed by incoming requests. This is especially important when the Taurus producer is busy processing pending transactions or the oracles are busy processing the oracle side workloads, as it ensures that new incoming

transactions from the oracles or events from the Taurus do not stall, thus maintaining a smooth operational flow. The 'reply-to' mechanism in RabbitMQ supports a responsive communication channel back to the oracles, providing them with transaction execution results, thereby enhancing interactive data handling.

The scalability of RabbitMQ allows Taurus to manage an increasing volume of transactions and event messages efficiently, without a proportional increase in the direct processing load on the core blockchain components. By decoupling the transaction input and event output processes from the core transaction processing units, RabbitMQ enhances the reliability and independence of the system. Each component can operate and recover from failures independently, which adds robustness to the Taurus architecture and offers extensive customization and configuration options to optimize performance and reliability according to the platform's needs.

- RESTful interfaces: Taurus offers a RESTful interface for stateless queries, which is scalable and easy to integrate with client systems. This interface supports high-volume and concurrent queries, crucial for large-scale enterprise operations.

These interfaces ensure Taurus can handle diverse workloads effectively, serving multiple clients simultaneously.

3.3 Taurus components

Taurus's architecture includes several critical components, each configured to perform specific functions:

- Block producers

  High Availability (HA) configuration: Multiple block producers are set up in a standby configuration, using a Raft-based consensus mechanism to manage quorum-based block commitments and handle failover seamlessly. This redundancy ensures that the blockchain maintains operation without a single point of failure.

  Transaction queuing and continuity: Transactions awaiting processing are queued, allowing the next active producer to seamlessly pick up processing without any loss of data or functionality, enabling continuous operation.

  Optimized performance: The primary active producer operates under semi-static configuration optimized for low latency and high throughput, critical for handling Bullish's demanding transaction loads. The transaction execution order is strictly determined by their arrival in the input queue, providing process integrity and consistency.

  Security and data integrity: The active producer also plays a crucial role in capturing and securing critical business data on-chain in real-time, providing traceability, immutability, and auditability for all transactions.

- Block sync service: This service reduces the burden on block producers by managing the distribution of blocks to various network nodes, supporting data consistency and high availability across the network.
- Streaming and query services: Comprising dedicated nodes equipped with streaming and query plugins, these services handle extensive data requests and event streaming. They are designed for high efficiency, allowing seamless data integration with external applications.
- Backup service: An automated backup system regularly secures critical data, safeguarding against potential data loss or corruption and ensuring that essential business information remains protected.
- Hardened validator nodes: These nodes in secured VMs with isolated and protected execution provide an additional layer of security by re-validating transactions and blocks, ensuring that all network operations adhere to the highest security standards.

3.4 Developer tools

To facilitate smart contract development, testing, and deployment, Taurus offers an array of tools:

- Contract development tools: The Contract Development Toolkit (CDT) including the extended standard libraries with backwards compatible and large scale enterprise application friendly data structures support facilitate the streamlined creation and deployment of enterprise business smart contracts, so that they seamlessly integrate with existing systems.
- Testing and debugging: Developers can utilize a sandbox environment to test and debug smart contracts in a controlled setting that emulates production conditions, mitigating risks associated with direct deployment.
- Operation and management: Through Cleos, a command-line tool, developers and administrators can efficiently manage network parameters, smart contract deployments, and other operational configurations, for smooth and secure blockchain operations.

The ongoing development and strategic enhancements of the Taurus architecture demonstrate Bullish's proactive approach to leveraging cutting-edge technology. This commitment ensures Taurus is not only prepared to handle current operational demands but is also well-equipped to adapt to emerging blockchain innovations.

4. Ensuring data security with Taurus

Security within the Taurus blockchain architecture is underpinned by robust measures designed to protect data integrity and prevent unauthorized access. This section outlines the key strategies employed to secure the blockchain environment.

4.1 Protected signing keys

The security of transactions and blocks within Taurus hinges significantly on the integrity of the signing keys. These keys are crucial as they validate the authenticity of each transaction processed through the blockchain. Taurus

employs several methods to secure these keys based on their usage and criticality:

- Hardware-level non-extractable keys: For signing blocks and key business transactions, Taurus utilizes non-extractable keys generated and stored within secure hardware modules. This approach prevents keys from being duplicated or extracted from their secure environment, providing confidence that signatures for transactions and blocks originate exclusively from authorized and secure sources.
- Cold storage and offline signing: Keys essential for critical operations, such as smart contract upgrades, are stored offline in cold storage environments. These keys are accessed only via air-gapped systems, which undergo rigorous security checks and are used solely for signing pivotal transactions under an operation procedure focusing on segregation of duties. This method significantly reduces the risk of unauthorized access and ensures that key actions within the blockchain are securely authenticated.

Together, these strategies are designed to ensure that all modifications to the blockchain state are securely authenticated, maintaining the integrity and trustworthiness of the entire blockchain infrastructure.

4.2 Validation everywhere

As a distributed ledger technology, the Taurus blockchain operates as a replicated deterministic state machine where consistency across all nodes is paramount. To this end, every node within the Taurus network is configured to independently validate each block it receives:

- Continuous validation cycle: The blockchain architecture incorporates a rigorous validation loop wherein every node continuously verifies and cross-checks the authenticity of transactions and blocks. This process allows any discrepancies or anomalies to be quickly identified and addressed.
- System resilience and security monitoring: If a potential compromise or anomaly is detected—whether in a block producer node or any other part of the network—affected nodes will halt synchronization and reject compromised blocks. This response prevents the propagation of potentially malicious data across the network, while automated alerts facilitate rapid response and investigation.

4.3 Hardened validation in a hardened environment

To bolster security further, particularly for transactions and activities that encompass critical business logic, Taurus leverages hardened validation environments:

- Secured Virtual Machines (VMs): Critical validation processes are conducted within Secured VMs that operate on an encrypted and tightly controlled infrastructure. These VMs ensure all data at rest and in use is encrypted, providing a fortified environment for transaction processing.
- Isolated and protected execution: Each Secured VM runs a hardened operating system that strictly controls

access to critical resources and ensures that only digitally signed applications and processes are executed. This layer of security is reinforced through a rigorous multi-team review and signing process, ensuring that only verified and secure code operates within these environments.

- Redundancy against compromise: In the unlikely event that primary systems are compromised, these hardened validator nodes stand as a robust last line of defense, capable of rejecting any transactions or blocks with invalid or altered signatures. This provides additional confidence that even in extreme scenarios, the integrity of the blockchain remains intact and the custody systems built on top and the managed customer assets are safe.

By implementing these sophisticated security measures, Taurus provides a secure and resilient platform for managing and executing transactions, so that all data handled meets the high-security standards required by Bullish's custody systems.

Conclusion

This post has detailed the architectural evolution and robust structuring of the Taurus blockchain, the backbone of high-performance, secure operations at Bullish exchange. Engineered to meet stringent security standards and performance demands, Taurus reinforces the foundation of 'Trust' essential to Bullish's operations.

Taurus's architecture exemplifies our commitment to security and reliability, from rigorous protection of signing keys to extensive validation processes and fortified environments for critical operations. These features are designed to ensure that every transaction is processed reliably and securely, fostering trust among users and stakeholders. This trust is reinforced by Taurus's adaptability and resilience in meeting the ongoing operational demands of the exchange environment, demonstrating high availability and comprehensive disaster recovery capabilities.

In subsequent posts, we will explore specific deployments of Taurus at Bullish, highlighting how our architectural choices and software modules of Taurus enhance system availability, disaster recovery strategies, and observability. These elements are crucial for maintaining uninterrupted service and operational integrity, ultimately ensuring continuous business operations.

By continuously refining the Taurus blockchain, we uphold our commitment to building and sustaining 'Trust'—both as a principle and in practice. This ongoing effort not only meets Bullish's operational needs but also sets benchmarks for security, performance, and reliability within the broader blockchain community.

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**.

[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.

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