FILENAME CONTROL PLANE SECURITY FOR BLOCKCHAIN

Establishing True File Identity Across Blockchain, PKI, and File Containers

Abstract v1.1

Blockchain and PKI establish when data existed and who approved it, but neither defines what a file actually is in its operational context. This paper introduces VeraFile as the missing identity layer, binding filename and content into a single verifiable construct so blockchain can anchor true, context-aware file identity.

VeraSec Technologies

About VeraSec Technologies LLC

VeraSec Technologies is a pioneer in Artifact Identity Security (AIS), focused on moving the security context from the infrastructure directly to the file itself. While traditional security models rely on centralized systems to establish and maintain trust, VeraSec's patent-pending technologies empower files to carry their own verifiable identity - preparing them for an actual Zero Trust world.

Operating at the forefront of Portable File Identity (PFI) technology, VeraSec invented the Validation Integrity Key (VIK) process. This innovation patches a fundamental vulnerability in traditional PKI that has persisted for decades. By cryptographically binding a file's content and metadata into a compact, human-readable identifier embedded directly within the artifact, VeraSec helps organizations set up durable, portable trust in every digital asset, signed or un-signed - wherever it travels.

About The Publisher

Brian Hajost (bhajost@verasec.net) is a cybersecurity entrepreneur and technologist with more than 30 years of experience in information security, compliance automation, and trusted computing systems.

As the founder of SteelCloud, he pioneered the automation of DISA STIG and CIS benchmark compliance for the DoD, federal agencies, and enterprise customers. Brian holds 15 patents in information technology and mobile security. In 2022 he was named one of the "Top 10 Most Influential People in Cyber Security" by CIO Views.

His current work focuses on solving what he describes as the Artifact Identity Problem - the absence of durable identity for files as they move across distributed infrastructures and untrusted networks.

Filename Control Plane Security for Blockchain

Establishing True File Identity Across Blockchain, PKI, and File Containers

Executive Summary

Blockchain technology has fundamentally reshaped how organizations establish trust in distributed environments. By providing an immutable, decentralized record of events, it enables verifiable timelines without reliance on centralized authorities. When applied to file integrity, blockchain is used to notarize cryptographic hashes, creating a durable proof that a given dataset existed at a specific moment in time.

This model is powerful - but incomplete. Blockchain proves that something existed. It does not prove what that thing actually is.

The limitation lies in the fact that blockchain anchors to hashes, and hashes anchor to raw data, but neither binds to the contextual identity of a file and how it is used in human workflows. At the center of this gap is the filename - the primary mechanism through which systems and users assign meaning to data - which remains entirely outside the cryptographic boundary.

VeraFile introduces a missing identity layer that allows blockchain to anchor not just data but meaning. By binding filename and content into a single, verifiable construct through Validation Integrity Keys (VIKs), VeraFile transforms blockchain from a passive timestamping mechanism into a system capable of securing true file identity. When also integrated with Public Key Infrastructure (PKI) and extended across complex file containers, this model establishes a complete and durable framework for digital provenance.

This white paper outlines the integration of VeraSec's VeraFile technology as the foundational Identity Layer for blockchain. Utilizing an optional High-Trust, Split-Node architecture, nested ZIP containerization, and a modular Four-Tier provenance model, organizations can enforce absolute file identity without compromising legacy compliance or introducing the operational friction of endpoint key management.

Blockchain's Promise - *and Its Structural Limitation*

Blockchain systems are designed to establish consensus around the existence and ordering of events. In file integrity use cases, this is typically achieved by recording a cryptographic hash on-chain, often accompanied by metadata such as timestamps,

transaction identifiers, or ownership attributes. If a file's hash matches the value stored on the ledger, it can be said to have remained unchanged since notarization.

However, this assurance is limited to the integrity of the byte sequence itself. It does not extend to the meaning of that data within the systems that consume it. A hash is inherently context-free; it does not encode how a file is named, how it is intended to be used, or how it is interpreted by downstream processes.

This creates a structural disconnect. A file may be perfectly valid from a cryptographic standpoint - its hash matches, its ledger entry is intact, yet its operational meaning may have been altered entirely. Renaming a file, repositioning it within a workflow, or embedding it in a different execution context does not change its hash, but it can radically change its behavior and perceived purpose.

Blockchain secures data but remains blind to identity.

The Filename Control Plane

In modern enterprise environments, filenames are far more than descriptive labels. They function as control signals that influence automation, dictate execution paths, and guide human decision-making. Systems routinely rely on filenames to determine how data should be processed, trusted, or ignored.

Despite this, filenames remain outside the scope of traditional security controls. They are treated as mutable metadata, rather than as a critical component of operational trust. This creates a persistent vulnerability: the ability to manipulate how a file is interpreted without altering the file itself.

This layer - the interface between raw data and operational meaning, can be understood as the Filename Control Plane. It is where files acquire their identity in practice, and it is precisely the layer that existing cryptographic systems fail to secure.

Until this plane is brought within the trust boundary, blockchain-based validation will continue to certify data that may no longer represent what it claims to be.

VeraFile: *Enabling Identity-Aware Blockchain*

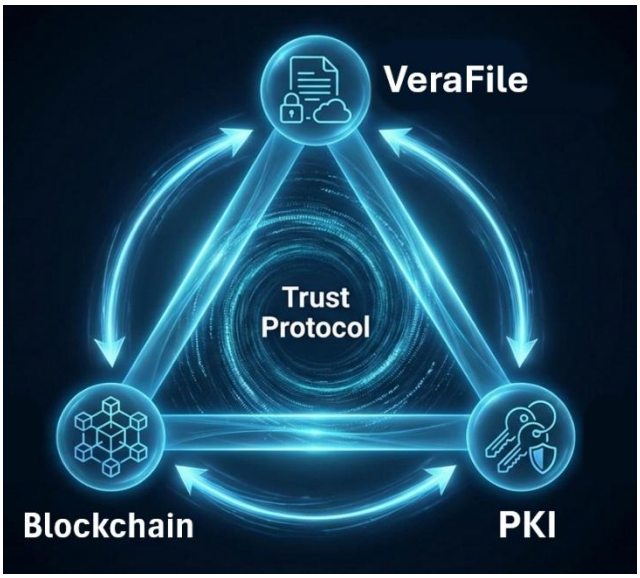
VeraFile introduces a mechanism that allows blockchain to anchor true file identity rather than abstract data. At the center of this model is the Validation Integrity Key *(VIK)*, which binds a file's contents, filename, and structural attributes into a single, inseparable identity.

Unlike traditional hashes, which are deliberately indifferent to context, the VIK incorporates the filename directly into its derivation. This ensures that any change to either the data or its representation results in a new identity. The file can no longer be separated from how it is presented to systems or users.

When a VIK is recorded on a blockchain, the ledger is no longer referencing a context-free dataset. It is anchoring a fully defined artifact, one whose meaning is cryptographically enforced. This transforms blockchain from a system that records existence into one that also records identity.

Integrating Public Key Infrastructure *(PKI)*

While blockchain establishes temporal integrity and VeraFile establishes contextual identity, Public Key Infrastructure continues to play a critical role in binding human or organizational intent to digital artifacts. PKI answers the question of authorship - who approved or signed a file, but it does not inherently ensure that the file's identity remains stable after signing.



In traditional implementations, PKI signatures are often applied to portions of a file or to representations that can be altered without invalidating the signature in a meaningful way. This creates opportunities for what can be described as signature laundering, where a valid signature is preserved while the surrounding context is manipulated.

By introducing VeraFile into the process, PKI signatures become anchored to a stable identity. The VIK ensures that the filename and content cannot be altered without detection, meaning that the scope of what is being signed is effectively expanded to include the file's full operational context. Any attempt to rename, repackage, or remove and/or replace the PKI signature, invalidates the file's VIK integrity and trustworthiness of the associated signature.

This alignment creates a cohesive model in which PKI, blockchain, and VeraFile each reinforce one another. PKI establishes who approved the artifact, blockchain establishes when it existed, and VeraFile ensures that both of those assertions apply to an immutable, context-bound identity.

Extending Trust to Containers with Cryptographic Bills of Materials

Enterprises rely heavily on containers - archives, document bundles, and other multi-component artifacts, that introduce significant complexity into integrity validation. In blockchain-based models, flat files typically require a separate JSON ledger *(sidecar)* to represent their state. Containers, such as ZIP archives, are therefore often used to consolidate the file and its associated ledger into a single transportable unit, simplifying handling and distribution. However, this approach exposes a fundamental limitation: traditional hashing methods are not reliable in non-canonical formats like ZIP, where identical content can yield different hash values based on file ordering, compression, or metadata.

As a result, conventional hash-based validation cannot consistently distinguish between benign structural variation and meaningful tampering. VeraFile addresses this challenge through a hierarchical identity model that extends trust across the entire contents of a container. To secure these assets, the architecture pivots to a robust nested ZIP container approach:

- **Component Sealing:** Individual VIKs are generated for the core files, the ledger JSON intent, and any optional detached PKI signatures.
- **Manifest Generation:** VeraFile creates a JSON manifest which inventories the components, files, sidecars, PKI signatures, and their first-tier VIKs. A second-tier VIK seals this manifest itself, locking the internal component relationships.
- **Container Sealing:** The components and manifest are compressed into a ZIP envelope, sealed with a final Container VIK, immutably locking the relationship between ZIP components and its ledger intent. Only this outer VIK requires ledger notarization.

During endpoint execution, a container Nested Processing routine validates the outer container against the ledger, extracts the manifest, and validates the individual executable at the exact millisecond of access, eliminating the extraction vulnerability window. Because of the cascading cryptographic relationship, validating that single ledger entry mathematically proves the integrity of the manifest, which in turn proves the integrity of every extracted component inside. And VeraFile builds the inventory manifest and seals each component.

This is where blockchain integration becomes strategically powerful. By anchoring the Container VIK to a public blockchain such as Ethereum, the entire multi-component artifact, regardless of internal complexity, is reduced to a simple, immutable external

reference. This anchor provides an independently verifiable timestamp and proof that the exact artifact identity existed at a specific moment in time.

Importantly, VeraFile does not rely on blockchain to function. The container remains fully self-validating and portable without any external dependency. Blockchain serves as an optional notarization layer, extending trust beyond the enterprise boundary by enabling third parties to verify not only that the artifact is intact, but that its identity was established and committed at a known point in time.

The result is a dual-layer trust model. VeraFile ensures that the container proves itself wherever it travels, while blockchain anchoring allows that proof to be independently validated and historically fixed. Together, they establish a true cryptographic chain of custody for containerized data, where every component is verifiable, every relationship is sealed, and the entire system is both portable and externally attestable.

The Four Tiers of File Provenance

VeraFile anchors file identity as a first-class security primitive, enabling enterprises to layer blockchain, PKI, and file containerization into a flexible, value-driven secure architecture.

Tier 1: ***Base Identity (VeraFile)***

- Use Case: *Autonomous logs, high-volume operations, standard office documents.*
- Value: *The VIK binds filename to contents, defeating renaming attacks with fast, keyless, file integrity.*

Tier 2: ***Distributed Provenance (VeraFile + Blockchain)***

- Use Case: *Audit trails, external sharing, high volume artifact production.*
- Value: *Proves identity and the exact time it existed, anchoring the VIK to an immutable distributed ledger. And, sealing the blockchain JSON data and the unique file name.*

Tier 3: ***Actor Non-Repudiation (VeraFile + PKI)***

- Use Case: *Executive approvals, classified signoffs.*
- Value: *Proves who approved the data, while the VIK ensures the context (filename) of that approval cannot be altered and the PKI signature cannot be removed and/or replaced without a validation failure alert.*

Tier 4: ***Absolute Provenance (VeraFile + PKI + Blockchain)***

- Use Case: *Highest value artifacts, legal contracts, intellectual property transfers.*
- Value: *The full chain of trust - binding actor, time, and immutable file identity into a single, verifiable truth.*

The "Two-Step Commit" Architecture: *Synchronizing Identity and Ledger*

Integrating identity-aware files with blockchain introduces a sequencing requirement that must be addressed. Because the VIK reflects the complete and final state of a file, any metadata associated with the blockchain transaction must be embedded prior to identity generation.

This is achieved through a two-step commit process. First, relevant ledger intent - such as smart contract references or organizational identifiers, is inserted into the file. The file is then sealed through VIK generation, which binds the finalized contents and filename into a single identity. Both the artifacts container VIK and contents hash are then submitted to the ledger in a unified JSON payload.

This sequence ensures that the blockchain entry corresponds exactly to the file as it exists in practice. There is no divergence between what is recorded and what is validated. The ledger becomes a precise anchor for a fully realized digital artifact.

Reconciling Identity with Compliance Requirements

Enterprise adoption of blockchain and advanced identity models must coexist with established compliance frameworks, many of which mandate the use of standard cryptographic hashes. VeraFile accommodates this requirement by generating both a traditional content hash and a composite VIK for each sealed file.

Both values can be recorded on-chain, allowing organizations to satisfy regulatory expectations while simultaneously enforcing a higher standard of integrity. The hash provides continuity with existing audit practices, while the VIK delivers the contextual assurance required for Zero Trust environments.

This dual-record model ensures that enhanced security does not come at the expense of compatibility or compliance.

Conclusion

Blockchain has established itself as a powerful mechanism for recording immutable facts about data. PKI has long provided a means of binding identity to action. Yet both have operated under an implicit assumption: that the data being validated is inherently meaningful and stable.

In practice, this assumption is flawed.

The meaning of a file is inseparable from how it is named, interpreted, and used. By leaving this dimension unprotected, traditional approaches to file integrity allow critical gaps to persist, gaps that can be exploited without violating any cryptographic guarantees.

VeraFile closes this gap by introducing identity as a first-class element of trust. By binding filename and content into a single construct, it enables blockchain to anchor not just data, but meaning, and allows PKI to bind intent to a truly stable artifact.

The result is a unified model of digital provenance in which identity, time, and authorship are aligned to a single, immutable reference point.

- ✓ Blockchain proves when something existed.
- ✓ PKI proves who approved it.
- ✓ VeraFile ensures you know exactly what it was.