

HASHORIGIN™ TECHNOLOGY

HashOrigin™: cryptographic assurance for every document

How Twala seals, fingerprints, and anchors every completed document so that anyone holding a copy can confirm it is genuine and unchanged, without relying on Twala as a single point of trust.

■ CONTENTS

HashOrigin™

01	Executive summary	3
02	The problem HashOrigin solves	3
03	How HashOrigin works: five stages	4
04	What each layer proves	6
05	Built on international standards	6
06	Seals for every kind of organization	7
07	Verification for recipients	7
08	What HashOrigin is designed to do	8
09	The platform around HashOrigin	8
10	Strategic value	9

■ ABOUT THIS PAPER

This paper explains HashOrigin™, the trademarked technology under every document Twala seals: the problem it solves, its design goals, the five stages from seal to verification, the international standards it is built on, the seal tiers available to organizations, how recipients verify documents, what each layer proves, the platform security around it, and its strategic value to Twala.

■ THE TWALA WHITEPAPER SERIES

No. 01
Company profile

No. 02
Use cases: context-aware workspaces

No. 03
eNotary

No. 04
eSignature

No. 05
Document intelligence with Lex

No. 06
HashOrigin™

■ 01

Executive summary

For a digital document, the question that matters is never whether it looks right. It is whether this is exactly the file that was signed or notarized, down to the last byte.

HashOrigin™ is the trademarked technology under every document Twala seals: envelopes signed with eSignatures, timestamped files, and every eNotarized document. It answers that question in two independent ways.

A seal inside the file

A digital signature made with Twala's X.509 certificate covers the finished PDF, with a trusted timestamp and long-term validation evidence. Change anything and the seal no longer matches.

A fingerprint outside the file

The sealed document's SHA-256 fingerprint is anchored on a public blockchain, where it cannot be altered. Anyone can check a copy against it, with or without Twala.

5

Stages: seal, fingerprint, batch, anchor, verify

2

Independent proofs for every document

15 min

Interval at which fingerprints are anchored

0

Document contents or personal data written on-chain

HashOrigin has its own dedicated home at hashorigin.io, which publishes anchor proofs, details of the contracts Twala anchors on, and a sample verifier for anyone who would rather check than trust.

■ 02

The problem HashOrigin solves

A paper document is hard to copy perfectly but easy to alter in small ways: a figure changed with correction tape, a page swapped before the staples go in. A PDF has the opposite profile. Perfect copies cost nothing, and an edit leaves no trace on the page. The Supreme Court itself has recognized how easily third parties can fake notarial seals and stamps.

As contracts, affidavits, and powers of attorney move online, the institutions that receive them, such as banks, registries, courts, employers, and government offices, need to confirm authenticity at the counter, in seconds, from the file itself. HashOrigin is designed for exactly that moment.

DESIGN GOALS

Tamper-evidence

Any modification to a document, however small, is immediately detectable.

Independent verifiability

Third parties can verify integrity without relying on Twala as a single point of trust.

Long-term validity

Proof that stays checkable for decades, after certificates expire and systems change.

Privacy

Only fingerprints are anchored.
Documents and personal data
stay in the customer's workspace.

Interoperability

Built on international standards
that PDF readers and public
blockchain tools already
understand.

Legal alignment

Designed around the Electronic
Commerce Act, the Rules on
Electronic Evidence, and the
Rules on Electronic Notarization.

■ 03

How HashOrigin works: five stages

HASHORIGIN IN FIVE STAGES



FIGURE 1 Every document Twala seals passes through the same five stages.

1. Seal the finished file

When a document is completed on Twala, whether it was signed, timestamped, or notarized, it is first converted to **PDF/A-2b**, the archival PDF standard (ISO 19005-2), so it renders identically for the long term. Twala then signs it with the **Twala Platform Seal**: a digital signature over a SHA-256 digest of the finished PDF, made with Twala's private key and backed by an X.509 certificate from Twala's own certificate authority. The Platform Seal is applied last, after the organization's own seal when the team has one, so it covers every signature on the document.

Each signature carries a trusted timestamp under **RFC 3161**, which fixes when it was made. When every signature on a document has it, **long-term validation (LTV)** evidence is embedded as well, the certificate chain and its revocation status at signing, so the signatures remain checkable after their certificates expire.

2. Take the fingerprint

Twala then computes the **SHA-256** hash of the sealed file and records it. The hash is a fixed-length fingerprint, 64 characters calculated from every byte of the file. The same file always produces the same fingerprint, and changing a single character changes roughly half of its 256 bits. The calculation runs only one way: the fingerprint reveals nothing about what the document says, which is why fingerprints, never documents, are what gets anchored.

3. Batch the fingerprints

Every 15 minutes, Twala gathers the fingerprints recorded since the last run into a **Merkle tree**. The fingerprints are paired and hashed together, then the results are paired and hashed again, level by level, until a single value remains: the Merkle root. That root stands for every document in the batch, while each document keeps its own

anchor proof, a short trail of neighboring values that leads from its fingerprint to the root. Alter the document and the trail leads somewhere else.

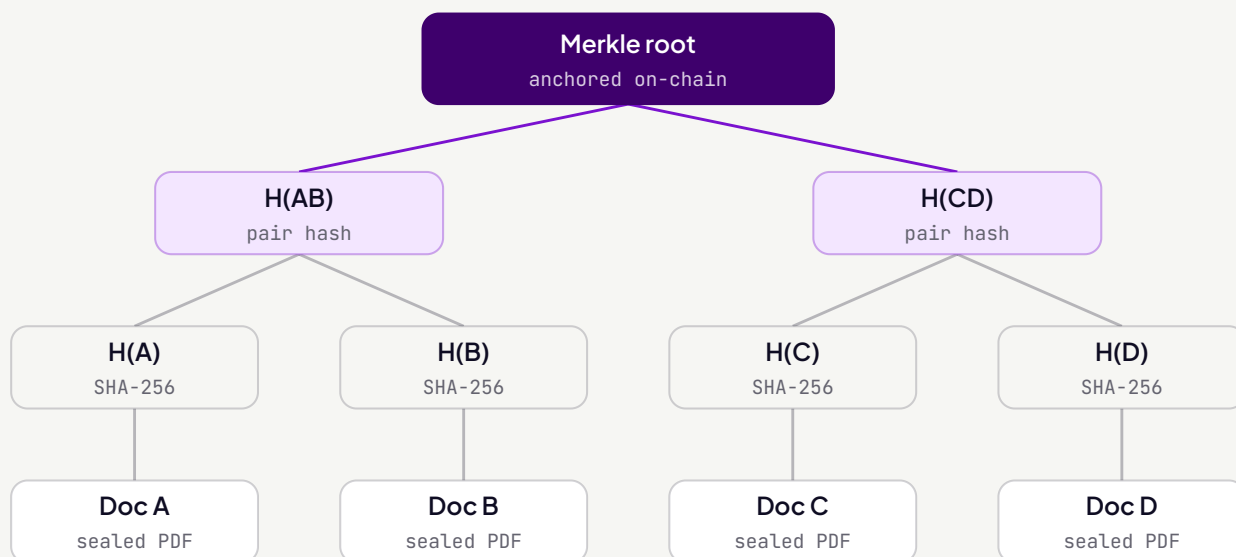


FIGURE 2 A simplified Merkle tree of four documents. Each document can be proven on its own by following its trail to the anchored root.

4. Anchor the root on a public blockchain

The Merkle root is written to Twala’s smart contract on a public blockchain, in a transaction of its own. The contract stores each root with the time of its block, and anyone can ask it whether a root was anchored and when. Once recorded, the root cannot be altered, and every block produced afterward makes the record harder to dispute. Any anchoring job that fails is retried automatically.

Nothing about the documents themselves is written to the chain: no names, no contents, and no personal data, only a fingerprint of fingerprints. That is how a public blockchain can hold the proof for contracts, affidavits, and powers of attorney while keeping every one of them private.

5. Verify, with or without Twala

Anyone holding a copy can check it on Twala’s verify page. The page computes the file’s fingerprint, finds it in Twala’s records, shows the Merkle root and the block where the root was anchored, checks the seal’s certificate against Twala’s trust registry, and returns a verdict: **Document verified**, or **Document tampered** if anything changed after sealing.

The second check does not need Twala at all. With the document’s anchor proof, anyone can recompute the root with their own tools and compare it with what is recorded on the chain. A tampered document fails twice over: its digital signature no longer matches, and its fingerprint leads to a root the contract does not hold.

04

What each layer proves

LAYER	WHAT IT PROVES	HOW TO CHECK IT
Twala Platform Seal (X.509 digital signature)	The file has not changed since it was sealed	Twala's verify page, or the signature panel of a PDF reader such as Adobe Acrobat
RFC 3161 timestamp	When the seal was applied	The signature details in a PDF reader
Long-term validation evidence	The certificate was valid when the document was signed	Embedded in the signed PDF; read by PDF readers that support LTV
SHA-256 fingerprint and blockchain anchor	This exact file existed, unchanged, when its batch was anchored	Twala's verify page, or the anchor proof with independent tools
Notarial register and Central Notarial Database (eNotarized documents)	The notarial act was performed and recorded	The register entry on the notarial certificate page, and the Supreme Court's database

05

Built on international standards

STANDARD	ROLE IN HASHORIGIN
SHA-256	The document fingerprint: a cryptographic hash of the sealed PDF, recorded and anchored
Merkle trees	Efficient batching of many fingerprints, with an individual proof for each document
X.509 certificates	Behind the Twala Platform Seal and organization seals, readable by standard PDF readers
RFC 3161	A trusted timestamp from a timestamp authority inside each signature
PDF/A-2b (ISO 19005-2)	The archival format sealed documents are converted to before signing
Long-term validation	Certificate chain and revocation evidence embedded in the signatures
Public blockchain	A permanent, independently auditable record of each batch's Merkle root
TLS	Encryption in transit on every connection to the platform

Because HashOrigin is built on open standards, Twala documents work with tools organizations already use, from PDF readers that check digital signatures to public blockchain explorers. Twala is also a member of the **Cloud Signature Consortium**, the global organization that develops standards for cloud-based digital signatures, and its only Philippine member.

■ 06

Seals for every kind of organization

SEAL	AVAILABLE ON	PURPOSE
Twala Platform Seal	Every plan	Seals every completed document. Applied last, so it covers every other signature and seal on the file.
Business verified digital seal	Business, Business Plus, and Enterprise	The organization's own verified seal on the documents it sends, applied before the Platform Seal.
PKI digital seal	Enterprise	An organization-level PKI seal for institutions with their own certificate requirements.

WHERE HASHORIGIN APPLIES

eSignature envelopes

Every completed envelope is sealed and anchored, so even a routine approval carries digital-signature proof.

Timestamps

Documents can be sealed and anchored without signatures, to prove their exact form at a point in time.

eNotarized documents

Every notarized PDF is sealed and anchored, and carries a "Secured by HashOrigin" mark on its notarization.

■ 07

Verification for recipients

Institutions that receive Twala documents can write verification into their procedures. It is faster than inspecting seals under a lamp, and it detects alterations a person reading a printout would miss.

A FIVE-STEP ROUTINE FOR FRONTLINE STAFF

01 Ask for the PDF itself

The proof lives in the file. Have the sender email or upload the PDF, or open it on their own device. A printout or a photo is a picture of the document, not the document.

02 Check it on Twala's verify page

The page shows the document's proof of record, from fingerprint to anchor, and returns Document verified or Document tampered.

03 Look at the signature panel

A PDF reader that checks digital signatures confirms whether the file has changed since sealing and shows each signature's trusted timestamp.

04 Read the certificate page

For an eNotarized document, confirm the notary, the act, and the register entry, and compare names with the person in front of you.

05 Keep the PDF

File the original PDF/A document, so the copy in the case file stays readable and checkable for years.

When to look closer

- A “notarized” PDF with an image of a stamp and no digital signature.
- A file that the verify page cannot match, or a signature panel reporting changes after signing.
- Only a printout, a photo, or a screenshot when the sender cannot produce the file.
- An innocent re-save in another app also changes the fingerprint, so the first step is always to ask for a fresh copy downloaded straight from Twala.

08

What HashOrigin is designed to do

HashOrigin is deliberately precise about its role, which is what lets institutions rely on it.

Keeps documents private

The chain holds only a fingerprint of fingerprints. Files stay in the customer’s Twala workspace.

Complements the law

Legal validity comes from the Electronic Commerce Act, the Rules on Electronic Evidence, and the Rules on Electronic Notarization. HashOrigin makes the evidence easy to check.

Preserves the notary’s role

The Electronic Notary Public confirms who appeared and that they acted freely. HashOrigin proves the record of that act has not changed since.

Identifies the genuine copy

Anyone can copy a PDF. HashOrigin tells the recipient whether the copy in front of them is the genuine, unchanged one.

09

The platform around HashOrigin

HashOrigin protects the document. Twala’s defense-in-depth security program protects everything around it, combining technical controls, organizational policies, and continuous oversight.

Identity

Government ID and live face verification, two-factor authentication, single sign-on through SAML and OpenID Connect, and one sign-in at a time.

Access

Role-based permissions checked on every request, and workspaces that stay private until shared.

Encryption

HTTPS and TLS on every connection, and sensitive fields encrypted by the application before storage, with keys kept separate.

Integrity

An integrity-protected audit log, request tracing, document version history, and activity logs on every envelope and notarization.

Resilience

High-availability design with continuously synchronized data, automatic retries for background work such as anchoring, and formal Disaster Recovery and Business Continuity Plans.

Oversight

Real-time security monitoring, documented incident response, a Privacy Manual and Data Protection Officer, and an internal ISMS as Twala works toward ISO/IEC 27001.

■ 10

Strategic value

- **Trust as a product.** Twala takes its name from *tiwala*, the Filipino word for trust. HashOrigin turns that promise into something every recipient can check.
- **Verification as distribution.** Every verified document introduces Twala to its recipient, whether a bank, a registry, an employer, or a court.
- **Durable intellectual property.** HashOrigin™ is a Twala trademark with its own dedicated domain, hashorigin.io, built on six years of work on blockchain-backed digital signatures.
- **Research lineage.** Twala has built blockchain-backed signatures since its founding in 2020 and keeps a research and development partnership with the Department of Science and Technology's Advanced Science and Technology Institute (DOST-ASTI).
- **Readiness for institutional acceptance.** As the Supreme Court's circulars with the Land Registration Authority and the Securities and Exchange Commission bring eNotarized documents into registries and regulators, a verifiable record is what makes acceptance at the counter practical.

"We built Twala so a document never has to leave the platform to be trusted. It's drafted, signed, notarized, and sealed in one place."

Alexander Paul Quinit, Co-founder and Chief Technology Officer

■ ABOUT TWALA

Twala is a Philippine legal technology company and a Supreme Court–accredited Electronic Notarization Facility (ENF). Its platform brings AI contract generation and review, eSignature, electronic notarization, and secure storage together, with every document sealed and independently verifiable through HashOrigin™ technology. Founded in 2020 and operated by Ohelio Inc., Twala serves more than 600 companies and 1.3 million individual users. Twala is backed by DOST-PCIEERD through its Startup Grant Fund Program and is a member of the Cloud Signature Consortium.

■ CONTACT

For investor relations, partnerships, and enterprise inquiries, email info@twala.ai or visit twala.ai.

Book a demo, explore pricing, or verify a Twala document at twala.ai. Technical details of HashOrigin™ are at hashorigin.io.

This whitepaper is provided for information purposes only and does not constitute an offer of securities or legal, financial, or investment advice. Figures are as published by Twala as of October 2026. Statements about plans, products in development, and expected outcomes are forward-looking and may change. Twala is a technology provider and does not give legal advice. Notarial acts are performed by commissioned Electronic Notaries Public. HashOrigin™ is a trademark of Ohelio Inc. Other names are the property of their respective owners. © 2026 Ohelio Inc.