



VERIFIED. RECORDED. IMMUTABLE.

Every agreement *set in immutable ink.*

Benjamin A. Aiello

benjamin@inkset.io

www.inkset.io

Table of contents

1	Abstract	03
2	Introduction	04–05
3	Problem statement	06
4	Solution overview	07
5	Technology	08–12
6	Use cases	13
7	Market opportunity	14
8	Roadmap	15
9	Conclusion	16

Making execution as verifiable as intent.

Agreements are how people and institutions exchange obligations, assets, and trust. The way they are executed has changed little since the U.S. E-SIGN Act gave electronic signatures legal standing in 2000. Documents still circulate as PDFs, identity is established by an email address, and the record of what happened is held by whichever vendor processed the signature. These systems are slow, costly to operate, and increasingly easy to defeat.

Inkset is a contract-execution platform built to close that gap. Every agreement on Inkset carries three guarantees. Each participant is verified through government-grade KYC/KYB. Each signature is produced by a cryptographic key bound to that verified identity. Each material event is recorded on the Arbitrum blockchain, secured by Ethereum, where it cannot be altered after the fact. Smart contracts will govern how an agreement progresses, so approvals, status changes, and signatures follow rules rather than reminders.

The platform is designed for multi-party transactions where proof matters long after the deal closes: real estate, private capital, family offices, legal services, and similar fields. Participants work in a familiar, collaborative interface. The blockchain operates underneath, with no wallets, tokens, or network fees to manage.

This paper sets out the problem Inkset addresses, the design of the platform, its technical architecture, the markets it serves, and the roadmap ahead.



Introduction

2.1 The state of agreement execution

Nearly every consequential transaction rests on an agreement. Agreements establish ownership, allocate risk, and define the terms on which parties rely on one another. Yet the tools used to carry them out have barely moved: a document is drafted in one system, emailed to counterparties, signed in another, and archived in a third.

The consequences are familiar to anyone who has worked a closing. Real estate transactions routinely run past a month. Venture and private equity rounds stall while signatures are chased. Sponsorship, transfer, and collective bargaining agreements are slowed by version confusion and disputes over who approved what. Every handoff between systems is a chance for a document to be altered or a party to be misrepresented.

2.2 A growing fraud surface

Fraud has followed those gaps. Wire fraud, title fraud, and impersonation schemes cost billions each year, and generative AI has lowered the barrier to entry. A synthetic identity, a cloned voice on a call, or a convincing forged closing statement can now be produced in minutes.

The standard response, adding intermediaries or layering on more approvals, raises cost and delay without addressing the core weakness. The parties still cannot prove who did what. Even in heavily regulated fields like real estate, banking, and labor, that weakness is tolerated as a cost of doing business.

2.3 An underused capability

Blockchain technology answers that weakness directly. A blockchain is a shared ledger maintained by many independent computers; once an entry is written, it cannot be quietly changed. Smart contracts, programs that run on that ledger, can enforce rules automatically and leave a verifiable trace of every step.

Most of the industry's attention, however, has gone to digital assets and trading. The ability to prove that an agreement was signed by the right people, in the right order, and never modified afterward remains largely absent from the tools businesses actually use.

2.4 Why we built Inkset

Inkset was built to put that capability to work on agreements. Every agreement, document, and milestone on the platform is governed by smart contracts and recorded on-chain. At the center is a signature engine that ties each signature to a verified person. The questions behind most disputes, who signed, when, and whether the document changed, now have answers that can be checked rather than argued.

The name reflects the idea. Iron gall ink goes on pale and darkens as it sets, and once set it cannot be lifted from the page. An agreement on Inkset moves the same way, from an editable draft to a permanent record.



OUR GOAL

Replace assumption with proof.
Every execution provable, every
identity verified, every step on
the record.

Problem statement

Five structural problems recur in how agreements are executed across industries.

3.1 Slow, fragmented processes

Complex agreements can take 30 to 45 days as documents move between disconnected tools and reviewers. A 2024 Deloitte and DocuSign study estimates that poor agreement management costs nearly \$2 trillion in global economic value each year.¹

3.2 High cost per agreement

Legal, administrative, and coordination overhead accumulates on every deal. World Commerce & Contracting estimates that weak contracting practices cost the average company 9.2% of annual revenue, rising to about 15% on large investment projects.²

3.3 Exposure to fraud

Without tamper-evident records or reliable identity checks, agreements invite manipulation and dispute. In Q1 2025, 46.8% of U.S. real estate transactions reviewed by FundingShield showed indicators of potential wire or title fraud.³ In a 2025 survey, 63% of REALTOR® association respondents were aware of title or deed fraud in their market, and 92% in the Northeast.⁴ Deloitte projects that U.S. fraud losses enabled by generative AI could reach \$40 billion by 2027.⁵

3.4 Poor integration

Few industries have standard, programmable infrastructure for executing terms. Organizations depend on intermediaries and insecure channels instead, and Gartner has found that nearly half of first-time contract lifecycle management (CLM) implementations fall short of expectations.⁶

3.5 Unequal access

Small and mid-sized firms are often shut out of secure automation by cost, technical complexity, and regulatory burden, which leaves them the most exposed to the risks above.

Sources. 1 Deloitte and DocuSign, 2024. 2 World Commerce & Contracting. 3 FundingShield, Q1 2025 Wire & Title Fraud Index. 4 National Association of REALTORS®, 2025 Deed & Title Fraud Survey. 5 Deloitte Center for Financial Services, 2024. 6 Gartner.

Solution overview: *proof built in*

Inkset provides a single, verified environment, called a room, in which an agreement is drafted, negotiated, signed, and permanently recorded. Each room holds the agreement's documents, its participants, and a complete history of every action. Six components work together inside it.

4.1 Verified identity layer

Every participant completes government-grade KYC/KYB and receives an identity-bound key before entering a room. No action is possible without it, preserving a continuous Chain of Identity.

4.2 AI Composer

Users describe a deal in plain language and Inkset drafts the agreement from their template library, capturing terms, parties, and obligations as structured data. Inkset AI suggests; a person accepts.

4.3 Smart contract automation

Status changes, tasks, approvals, and signature checks are governed by smart contracts, replacing manual coordination with rules that run the same way every time.

4.4 Cryptographic signatures

Each signature is generated by the signer's identity-bound key, establishing who acted, what they signed, and when, so only verified parties can take part.

4.5 Immutable audit trail

Agreements, documents, and signatures are recorded on-chain without personal data or direct identifiers, giving counterparties, auditors, and regulators a history they can check themselves.

4.6 Familiar experience

The blockchain runs beneath a conventional collaborative interface. Participants never manage wallets, hold tokens, or pay network fees.



5.1 Core architecture

The platform is organized in four layers, each with a distinct responsibility. Together they turn a signed agreement into a record that anyone with the right access can verify independently.



Signature layer

Signing runs in a custody-grade engine that confirms the full set of required, verified signers before an agreement can be set.

Execution engine

Smart contracts encode each agreement's conditions and advance it only when they are met. Approvals, milestones, and dependencies are checked automatically.

Audit layer

Every material event is written to the ledger. Each executed document's fingerprint is public, so its authenticity can be confirmed without an Inkset account.

Blockchain

Inkset is built on Arbitrum, a Layer 2 network that processes transactions quickly and settles them to Ethereum. This delivers confirmation in seconds, enterprise throughput, and the security of Ethereum's proof-of-stake consensus.

5.2 Identity verification: *knowing who is in the room*

Inkset establishes trust by confirming who is acting before anything else happens. Every participant, individual or organization, is verified and issued a cryptographic identity before entering a room. There is no guest signing.

Identity verification Verified · KYC/KYB

Individuals complete KYC and organizations complete KYB, confirming legal name, entity records, and professional credentials where relevant, with biometric authentication. The result is a persistent identity record tied to the account.

Key management

Each verified identity is paired with a unique cryptographic keypair: a public key others use to check a signature, and a private key used only to create one. Inkset holds private keys in isolated, encrypted custody, so participants never handle them.

Identity binding

Every action is signed with the participant's key and carries a reference to their verified identity. A signature cannot be detached from the person or entity that produced it, which closes the door on impersonation.

Roles and permissions

Access works in two layers. An organization role (Admin, Member, or Auditor) sets what a person can do across their company's rooms; Auditors are read-only and never see private drafts or AI conversations. A room grant (Owner, Editor, or Viewer) sets what they can do on their own side of a single room, and each side manages only its own grants. Signing is not a role: a signer badge marks the people in the signer set and works with any grant. Inkset AI takes part as a participant that suggests and never signs.

Every event on an agreement begins with a verified person, not an anonymous key.
This is the Chain of Identity.

5.3 Contract workflows

Each agreement on Inkset is represented by a set of smart contracts. A parent contract coordinates the agreement as a whole, each document carries its own on-chain record, and the full history is preserved on the ledger and in Inkset's indexed database. An agreement moves through three core states: Draft, In signature, and Verified.

STEP 01

Contract creation

A factory contract deploys a dedicated contract for the agreement, defining its collaborators, permissions, required steps, and current state. It coordinates the workflow establishes the smart contract which will parent the documents and signatures themselves.

STEP 02

Document registration

Each document gets its own blockchain record, linked to the parent contract and holding a cryptographic hash (a digital fingerprint) of the document. The hash is frozen at the first signature, so the document cannot change once signing begins.

STEP 03

Signature execution

Signers act at the document level through an on-chain transaction signed with their identity-bound key. Each is checked against the required signer list, and the hash and timestamp of every signature are recorded permanently.

STEP 04

Finalization

When the last signature lands, a final snapshot is written to the ledger, recording who signed, how they were verified, and what they signed. The agreement can be reconstructed and verified at any time afterward.

What the ledger holds, and what it doesn't

The ledger proves an agreement without exposing it.

What goes on-chain is the evidence: document fingerprints, signer addresses, signature events, timestamps, and the state of each agreement. What stays off-chain is the substance: document contents, deal terms, and KYC/KYB records, held encrypted and visible only to the parties in the room. A fingerprint reveals nothing about the document it came from, but it changes completely if a single character is altered.

5.4 Signatures compared: *a click, a certificate, a record*

Not every electronic signature carries the same evidence. Three approaches are in common use, and they differ in who vouches for the signer and where the proof is kept.

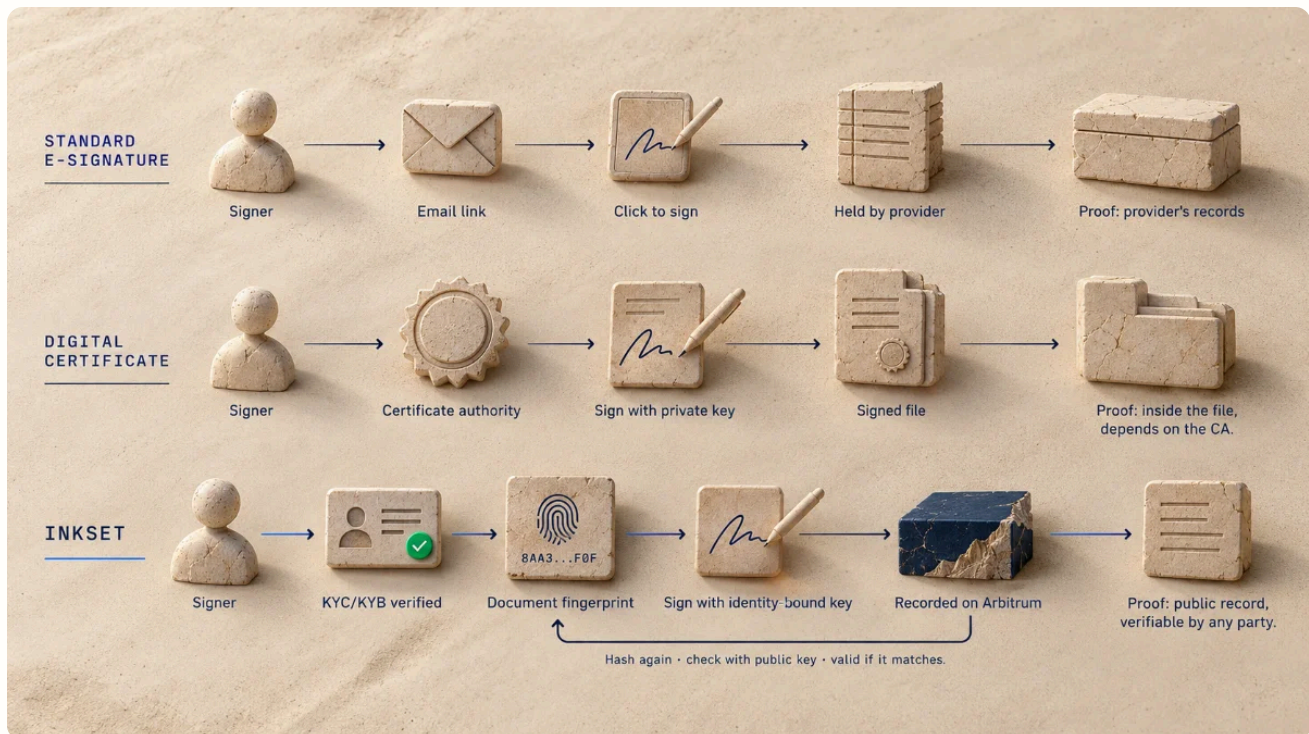


Figure 1. Three signature approaches, from signer to proof. A standard e-signature rests on inbox access and the provider's records. A certificate-based signature depends on a certificate authority, with proof inside the file. On Inkset, a KYC/KYB-verified signer signs the document's fingerprint with an identity-bound key, and the signature is recorded on Arbitrum where any party can check it.

Standard e-signature

The signer clicks a link sent to their email. Identity rests on inbox access, and the provider holds the audit trail and seals the file.

Digital certificate

A certificate authority vouches for the signer, who signs with a private key. The proof travels inside the file and depends on the authority.

Inkset

A KYC/KYB-verified signer signs with an identity-bound key. The signature is recorded on Arbitrum, where any party can check it without Inkset.

The difference shows over time. Provider audit trails last only as long as the provider and the account. Certificates expire and can be revoked, so checking an old signature means tracing the certificate chain back years. A record on a public ledger stays checkable by anyone, for as long as the network runs.

5.5 Where passkeys fit

Passkeys, built on the FIDO2 and WebAuthn standards and now supported by most phones and browsers, use the same publickey cryptography. The device creates a private key that never leaves it, and the website stores the matching public key. Signing in means proving you hold that private key. Passkeys are a strong replacement for passwords, but they are a different tool from an agreement signature.

Identity

A passkey proves control of a device, not who the person is.

Scope

Each passkey is tied to one website and used to log in, not to sign a document.

Record

A login leaves no shared or permanent record that a counterparty could check.

Inkset applies the same cryptography to the agreement itself. The key is bound to a KYC/KYB-verified identity, it signs the document's fingerprint, and the signature is recorded on a public blockchain.



Figure 2. Signature approaches compared. Many providers offer more than one; the columns describe the approach, not a single vendor.

Use cases: *where the record has to hold*

Inkset is designed for agreements with several counterparties, identity requirements, and records that must survive audits or disputes.

Real estate, closing, and escrow

Verified parties and tamper-evident documents remove the openings that wire and title fraud depend on.

Venture capital and private equity

Funding rounds and acquisitions with approvals captured in provable order.

Legal services

Wills, trusts, and case files with an independently verifiable chain of custody.

Entertainment and media

Licensing and sponsorship deals where rights and revenue change hands.

Family offices

Trust distributions and generational transfers with records that remain provable for decades.

Banking and lending

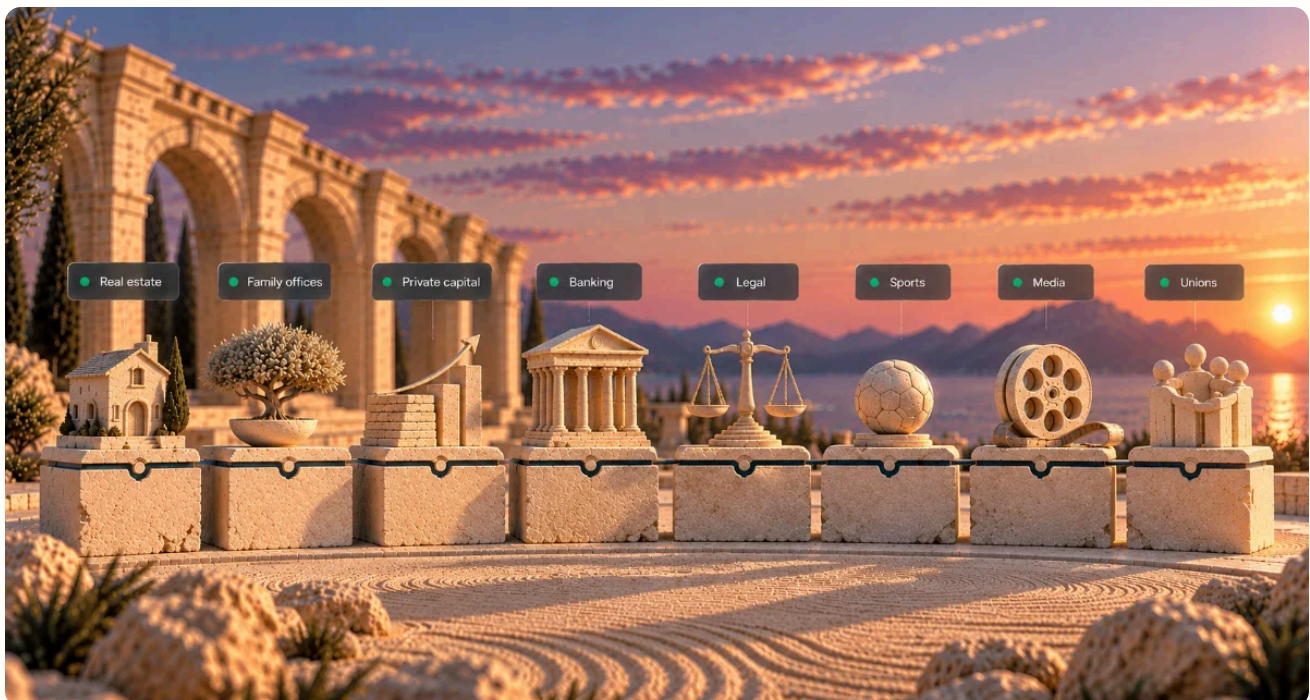
Loan documents and instructions backed by verified counterparties and exam-ready records.

Sports organizations and agents

Representation, transfer, and NIL agreements signed by the people they name.

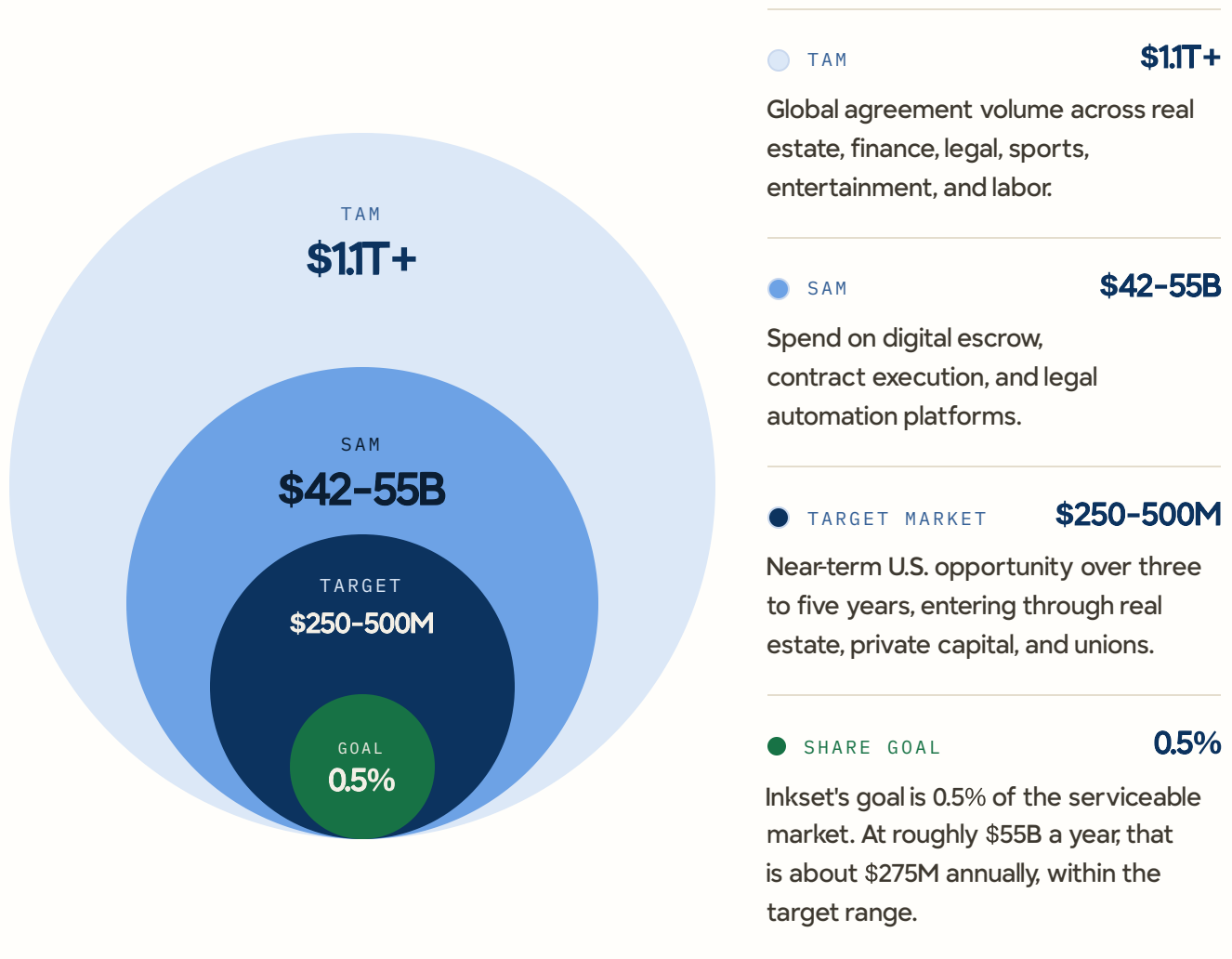
Unions and collective bargaining

Contracts and ratifications with verified signers and a permanent record of approval.



Market opportunity

Inkset sits where three established categories meet: escrow, contract execution, and legal automation. Each is large on its own, and each still relies heavily on manual process.



Real estate, private capital, and unions are the initial focus because they combine high transaction values, frequent multi-party signing, and well-documented fraud exposure.

Roadmap

Inkset is in its beta phase, piloting with early customers. The phases below reflect present plans and may change.

2025 Q4

COMPLETE

Phase 1 • Alpha

Foundation. Core agreement workflows, document handling, the first smart contract suite, and the initial interface.

2026 Q2 – 2027 Q1

IN PROGRESS

Phase 2 • Beta

In pilot with early customers. The cryptographic signature engine, local network integration, KYC identity verification, the Chain of Identity linking each verified person to their key, reporting and analytics, and smoother onboarding.

2027 Q2

PLANNED

Phase 3 • Private launch

Proving ground with select enterprises. Advanced smart contracts, testnet operations, DocuSign and Adobe Sign integrations, and the AI Composer for drafting and document parsing.

2027 Q3 – Q4

PLANNED

Phase 4 • Production

Goes live. Mainnet operations, advanced contract workflows, production acceptance testing, and full public launch.

2027 Q4+

PLANNED

Phase 5 • Fast follows

Beyond contracts. Extended third-party integrations, broader records infrastructure, and AI-driven fraud detection.

Conclusion

The weaknesses in how agreements are executed are well known: slow handoffs, unverified parties, and records that depend on trusting whoever holds them. Inkset addresses each one at the level of infrastructure. Participants are verified before they act, signatures are bound to those verified identities, and every material event is recorded on a ledger no single party controls.

The result is an agreement that carries its own evidence, from first draft to final signature, and remains verifiable long after the deal is done.



The ink sets, and so does the record.

Inkset is onboarding beta participants. To request a demo or join the beta, get in touch.

Benjamin A. Aiello

benjamin@inkset.io

www.inkset.io