MICKAI™

MICKAI EBOOK SERIES · No. 20

# The Provenance Standard.

Proving what a machine made: the right to be believed, and the record that earns it.

AUTHOR

**Micky Irons**

Founder and named inventor, Mickai LTD.

19 June 2026 · v1 · mickai.co.uk



Mickai LTD · Companies House 17166618 · press@mickai.co.uk · mickai.co.uk
UK IPO register, named inventor Mickarle Wagstaff-Irons · Trade mark UK00004373277

TABLE OF CONTENTS

# Contents

FOREWORD

# A note from the author

I have spent the last two years building a system whose entire reason for existing is that I no longer trust what I am looking at, and neither should you. A photograph is no longer evidence. A voice on a call is no longer the person you think it is. A video of a public figure saying something monstrous is, at this point, more likely to be fabricated than filmed. We crossed that threshold quietly, with no announcement, and most institutions have not noticed that the ground under them has gone. This book is my attempt to describe the only response I have found that actually holds, which is to stop trying to spot the fakes and start proving the genuine.

I am Micky Irons, founder and chief executive of Mickai, and I write this as a builder, not a commentator. Everything I argue here is implemented, filed, or running on hardware I can put my hand on. When I say a record can be sealed so that tampering becomes mathematically visible, I mean we built that seal and I can show you the audit trail. When I say provenance belongs at the point of creation rather than bolted on afterwards by a detector, I mean we put it there. I have no interest in selling you fear. The fear is already free and abundant. What is scarce, and what I want to hand you, is a method.

The argument is simple to state and hard to live by. Detection is a losing game because it is reactive, probabilistic, and always one generation behind the thing it is trying to catch. Proof is a winning game because it is affirmative, deterministic, and owned by the creator rather than the accuser. The future does not belong to whoever builds the best fake spotter. It belongs to whoever can point at their own work and say, here is the signed and anchored record that I made this, at this time, on this machine, and you can verify it yourself without trusting me. That is the right to be believed, and it has to be earned with a record.

I have tried to keep this honest. Where something is designed and filed but not yet hardened in production, I say so. Where the cryptography is settled and standardised, I say that too. The Sovereign Intelligence Operating System I describe is real, the fifty specialised brains run on the operator's own hardware and are fully offline-capable, and the sealing I lean on uses post-quantum signatures that are now a published federal standard. Read this as a working paper from inside the build, not a prophecy from outside it. If it changes how you think about a single photograph, a single recording, or a single piece of your own work, it will have done its job.

Micky Irons

Founder and named inventor, Mickai LTD · 19 June 2026

PART I · THE PROBLEM

# Why detection has already lost, and what we are actually defending.

## 1. The Collapse of the Default Trust

For most of recorded history a photograph carried a quiet presumption. Something stood in front of a lens and light fell on a surface, so the image was, broadly, a trace of a real event. That presumption was never perfect. People staged photographs, cropped them, retouched them and lied with captions. But the cost of a convincing forgery was high enough, and the skill rare enough, that the default ran the other way. We believed first and doubted on evidence. That default has now inverted, and the inversion is the single most important fact about the information environment we are all living in.

Generative models removed the cost. A photorealistic face, a cloned voice, a video of an event that never happened, all of these now sit a few seconds and a short prompt away from anyone with a browser. The marginal cost of a convincing fake has fallen to roughly nothing, and economics is merciless about things that cost nothing. They flood. When the supply of plausible falsehood becomes effectively infinite, the scarce resource is no longer the ability to produce an image. It is the ability to believe one. Attention did not become the bottleneck. Trust did.

> **We did not lose the ability to make images. We lost the ability to believe them, and that is a far more expensive loss.**

The damage is not only that bad actors can fabricate. It is subtler and worse. Once fabrication is cheap and known to be cheap, the genuine article loses its protection too. A real photograph of real wrongdoing can now be waved away as a probable fake, and the wave is plausible because fakes really are everywhere. This is the liar's dividend, the way a polluted information commons rewards the dishonest twice, once when they fabricate and again when they deny. The collapse of default trust does not merely admit lies. It corrodes the standing of truth.

I want to be precise about what has collapsed, because the precision points at the cure. What we have lost is not reality and not even our ability to record it. We have lost the link between a piece of media and a credible claim about its origin. The pixels are fine. The cameras are excellent. What is missing is a trustworthy answer to a single question asked of any artefact: where did you come from, and who will stand behind that answer. Everything in this book is an attempt to restore that one link, deliberately and verifiably, rather than to mourn a default that will not return.

## 2. Detection Is a Treadmill That Runs Backwards

The instinctive response to cheap fakes is to build a better detector. If a machine can make a synthetic face, surely a machine can learn to spot one. This is comforting, it attracts funding, and it is fundamentally a trap. Detection is reactive by construction. A detector can only learn the artefacts of the generators it has already seen. The moment a new model ships, or an old one is retrained against the detector itself, the artefacts shift and the detector's accuracy decays. You are not climbing a hill. You are running on a treadmill whose speed someone else controls, and they are speeding it up.

There is a deeper problem than lag, and it is structural. Modern generation is increasingly trained in an adversarial loop against exactly the kind of classifier a detector is. When the discriminator gets better, the generator is trained until it fools the improved discriminator, and then you ship the generator. The detector you build tomorrow is, in effect, a training target that makes the next generation of fakes harder to catch. Every detector you deploy publicly is a gift to the people you are trying to stop. This is not a bug in a particular product. It is the geometry of the contest.

## The asymmetry that never closes

Set the arms race aside and detection still fails on arithmetic. The defender must be right almost every time across an unbounded stream of content, while the attacker needs to succeed once against a specific target. A detector with ninety nine per cent accuracy sounds formidable until you point it at a billion items a day, where one per cent is ten million errors, a torrent of false accusations against the genuine and false clearances of the fake. Probabilistic verdicts on adversarial inputs at internet scale do not add up to trust. They add up to a confident-sounding noise generator.

Detection also answers the wrong question. It asks, is this fake, and returns a probability that no court, no editor and no ordinary person can actually rely on. The question that matters to a creator is different and far more tractable. It is, can I prove that this particular thing is mine and unaltered since I made it. That question has a clean answer that does not decay when a new model ships, because it does not depend on recognising the enemy at all. It depends only on a record that the creator controls. That is the pivot the rest of this book is built on.

The Mickai pantheon.

## 3. What We Are Actually Defending

Before designing any system it pays to say plainly what is under threat, because the threat is not the existence of synthetic media. Synthetic media is a tool, and I build with it daily. The thing under threat is provenance, the credible chain that connects an artefact to its origin and its history. When provenance fails, three concrete things break, and naming them keeps us honest about what a fix must actually deliver.

The first casualty is attribution. A creator can no longer reliably claim their own work, and an impostor can dress fabrication in a creator's identity. A cloned voice authorises a payment. A synthetic video puts words in a leader's mouth on the eve of an election. The harm here is not abstract reputational unease. It is fraud, defamation and the hijacking of identity at industrial scale, and it lands on individuals who have no detector and no recourse.

The second casualty is integrity over time. Even genuine media can be altered after the fact, a frame removed, a sentence spliced, a context stripped. Without a record of what the original was, there is no fixed point against which to measure the change. The third casualty is the one people feel without being able to name, the erosion of the affirmative. Honest people lose the ability to be believed even when they are telling the truth and holding the real thing in their hands, because there is no mechanism left that lets truth distinguish itself from a good forgery.

> **The goal is not to make fakery impossible. It is to make genuineness provable, so that the burden finally falls where it belongs.**

So the thing we are defending is the creator's standing to be believed, on their own evidence, without asking anyone to trust them on faith. That reframing matters because it changes the design target entirely. We are not building a wall against an infinite tide of fakes, which cannot be done. We are building a way for the genuine to carry a passport that the tide cannot forge. The rest of this book describes that passport, how it is issued at the moment of creation, how it is sealed so tampering becomes visible, and how it is anchored so that no single authority, including me, can quietly rewrite history.

PART II · THE PRINCIPLE

# Provenance is proof, issued at creation, owned by the maker.

## 4. Proof, Not Detection

The whole argument turns on a single inversion. Stop trying to prove that something is fake and start letting creators prove that something is genuine. These are not two routes to the same place. They are opposite in their mathematics and opposite in who carries the burden. Detection is a negative claim made about someone else's content by an outsider with incomplete information, and it degrades as generators improve. Proof is a positive claim made about your own content by you, the person who actually made it, with complete information, and it does not degrade at all because it never depended on recognising a forgery in the first place.

Consider how the two scale under pressure. A detector facing a smarter generator gets weaker. A proof facing a smarter generator is entirely unaffected, because a better fake does not weaken my signature on my real file. The strength of a proof depends on cryptography and on the discipline of capturing provenance at the right moment, not on the strength of the adversary's tools. This is why proof is the only approach that grows more valuable over time rather than less. The worse the fakes get, the more a verifiable genuine becomes worth, which is exactly the incentive structure you want a defence to have.

### The shape of an affirmative claim

An affirmative provenance claim has a specific anatomy. It binds an artefact to a set of assertions, who made it, with what tool, at what time, and after what edits, and it does so with a cryptographic signature that anyone can check and no one can forge without the private key. Crucially it is falsifiable in the honest direction. If a single bit of the artefact changes, the signature breaks and the verifier sees that it broke. The claim does not say trust me. It says check me, and here is the maths that lets you, and that distinction is the entire difference between marketing and proof.

This is why I built the Sovereign Intelligence Operating System around sealing rather than spotting. The SIOS does not try to be the world's best deepfake detector, because that race is unwinnable and I will not spend my operators' compute losing it. Instead every consequential action a brain takes is sealed into a record at the instant it happens, so that genuine output carries its own proof from birth. We are not in the business of catching liars. We are in the business of making honesty checkable, which is a far stronger position to hold and a far cheaper one to defend.

The Mickai pantheon.

## 5. The Point of Creation Is the Only Honest Place

Provenance has exactly one moment where it can be captured truthfully, and that moment is creation. Everything after creation is reconstruction, and reconstruction is guesswork dressed up as analysis. If you wait until an artefact is in the wild and then try to work out where it came from, you are an archaeologist sifting for clues, and a competent forger will have left you the clues they wanted you to find. Capture provenance as the file is made, by the tool that makes it, and there is nothing to reconstruct because the truth was written down while it was still true.

This is why a bolt-on detector can never be more than a stopgap. It arrives too late, downstream of every opportunity to lie. The honest place to assert who made this and how is inside the creating tool, at the instant of creation, before the artefact has had any chance to be copied, stripped or altered. The camera should sign the photograph as the shutter closes. The model should sign the generated image as the last pixel resolves. The recorder should sign the audio as the waveform is written. Provenance is a property to be minted, not a fact to be inferred.

> **You cannot reconstruct a truthful origin after the fact. You can only capture it at the source, or lose it forever.**

An honesty obligation comes with this, and I hold to it strictly. Capturing provenance at creation means telling the truth about creation, including when a thing is synthetic. A signed record that an image was generated by a model is not an admission of weakness. It is exactly the point. The provenance standard is not a badge that means real as opposed to fake. It is a faithful record of how a thing came to be, whatever that was. An honest signed disclosure that a model made an image is worth more than a thousand detectors guessing, because it is true at the source and it cannot be argued with.

This places a duty on tool builders, and I accept it as one of mine. If you build the camera, the model, the editor or the operating system, you are the only party positioned to capture provenance honestly, because you are present at creation and no one downstream is. Declining that duty and leaving provenance to downstream detectors is not neutrality. It is abdication, and it loads the cost of your convenience onto every honest creator who then cannot prove their own work. Building provenance in at the point of creation is the responsibility that comes with building the tools at all.

## 6. Sovereignty: The Maker Owns the Proof

A proof you do not control is not a proof. It is a permission, granted by whoever holds the keys, revocable at their convenience. This is the flaw I see in most provenance schemes on offer, which quietly route trust through a central platform that signs, stores and adjudicates on the creator's behalf. The creator ends up renting their own credibility. Change the platform's terms, lose the platform, or fall out with the platform, and your ability to prove your own work evaporates. That is not sovereignty. It is dependency wearing sovereignty's clothes.

The principle I build on is that the maker must own the proof outright. The signing key lives on the operator's own hardware, under the operator's own control, never escrowed to me or to anyone. The fifty specialised brains of the SIOS run on the operator's machine, fully offline-capable, precisely so that the act of creation and the act of sealing happen in a place the operator governs and no one else can reach. If the proof can only be made or checked by asking a third party for permission, then the third party owns your credibility, and one day they will price it accordingly.

### Local keys, portable proof

Sovereignty does not mean isolation. A proof generated on the operator's own hardware must still be verifiable by anyone, anywhere, without contacting the operator. That is the elegance of public-key cryptography rightly applied. The private key that creates the seal never leaves the maker's machine. The public key that checks the seal can be published to the whole world. So the maker keeps total control of the power to sign, while granting everyone the power to verify, and these two facts coexist without compromise. Owned creation, open verification, no trusted middleman in between.

This is the load-bearing wall of the entire design and I will not compromise it. Proof must be owned by the maker, sealed on the maker's hardware, and checkable by the world without anyone's permission. Anything less reintroduces exactly the central point of trust that the collapse of default trust should have taught us to fear. We are not replacing one set of gatekeepers with another. We are removing the gate. The record stands on cryptography and on a public anchor, not on anyone's institutional goodwill, and that is the only foundation I am willing to ask people to stand on.

The Mickai pantheon.

PART III · THE RECORD

# How a genuine artefact carries its own sealed, anchored proof.

## 7. Anatomy of an Open Audit Record

Everything so far has been principle. Now the mechanism. In the Sovereign Intelligence Operating System every consequential action is sealed into an Open Audit Record, and that record is the concrete object this whole book has been circling. An Open Audit Record is a structured, signed statement that binds an artefact to the facts of its making. It is not a wrapper around the file and it is not a watermark buried in the pixels. It is a separate, portable, cryptographically sealed document that says, in a form a machine can check, here is exactly what was made, by whom, when, with what, and after what steps.

### What the record actually contains

The record carries a cryptographic hash of the artefact, which is its fingerprint, so that any later change to even a single bit produces a different fingerprint and a broken seal. It carries the assertions of provenance: the identity of the creating brain or operator, the tool and model version, a timestamp, and an honest declaration of whether the content was captured or generated. It carries a record of transformations, so that an edit is not a silent erasure of history but an appended, signed entry that says this was changed, by this party, in this way. The record is a ledger of an artefact's life, not a snapshot of one moment of it.

The word open in Open Audit Record is deliberate and it is a commitment. The format is not a black box that only my software can read. The record is structured so that any compliant verifier can parse it, check the hash against the artefact, and validate the signature against a public key, with no dependency on Mickai's servers or goodwill. A proof that only its issuer can interpret is not a proof, it is a brand. We aligned the design with the direction the open content-provenance standards are travelling, because a record the wider ecosystem can read is the only kind that earns trust outside the walls of the system that made it.

Two properties make the record useful rather than decorative. It is tamper-evident, meaning you cannot quietly alter the artefact or the record without the seal visibly breaking. And it is self-contained, meaning the proof travels with the work and can be checked offline, without phoning home. Together these mean the genuine artefact carries its own evidence wherever it goes, into a courtroom, an editorial desk or a hostile feed, and that evidence speaks for itself without needing the creator present to vouch for it. That is what it means for a thing to be provable rather than merely asserted.

## 8. Sealing It So Tampering Becomes Visible

A record is only as trustworthy as the seal that protects it, and here the choice of cryptography is not a detail, it is the whole game. We seal every Open Audit Record with a post-quantum digital signature,

specifically ML-DSA-65 under FIPS 204, the signature standard the United States National Institute of Standards and Technology published in 2024. I will explain why each of those words is load-bearing, because the reasoning is the reassurance, and I would rather you understood the seal than merely trusted it.

A digital signature gives us exactly the two properties provenance demands. It proves origin, because only the holder of the private key could have produced the signature, and it proves integrity, because the signature is computed over the artefact's hash, so any change to the artefact invalidates the signature. Sign at creation and you bind the maker's identity and the artefact's exact state into one object that cannot be forged without the key and cannot be altered without detection. Tampering does not slip through. It announces itself by breaking the seal, which is precisely the behaviour we want.

### Why post-quantum, and why now

The reason for choosing a post-quantum scheme rather than a classical one is a problem with an ugly name: harvest now, decrypt later. An adversary can capture signed records today and wait for a sufficiently capable quantum computer to break classical signatures retroactively, at which point every record sealed with the old maths becomes forgeable after the fact. A provenance record is supposed to hold for decades, across legal, historical and archival timescales. Sealing it with cryptography that a future machine can quietly defeat would be building a vault with a lock we already know how to pick tomorrow. ML-DSA-65 is built to resist both classical and quantum attack, which is the only honest choice for a record meant to outlive the present generation of computers.

> **A provenance record must survive the machine that has not been built yet, or it is not a record. It is a postponed forgery.**

Standardisation matters as much as strength, and this is where I can be unusually concrete. ML-DSA-65 is not my private invention that you have to take on faith. It is a published federal standard, FIPS 204, scrutinised in the open by the world's cryptographers before it was finalised. That means a verifier does not have to trust Mickai's cleverness. They have to trust mathematics that has been examined far more harshly than anything I could produce alone. Sovereignty and openness meet exactly here: the key is mine and stays on my hardware, but the algorithm sealing the record is public, standardised and independently checkable, so the proof rests on no one's good name, least of all my own.


The Mickai pantheon.

## 9. Anchoring It So History Cannot Be Rewritten

A signature proves who made a record and that it has not changed. It does not, on its own, prove when. And time is where provenance is most often attacked, because the cheapest forgery is not altering content but backdating it, claiming a thing existed earlier than it did, or that an original came after the copy. To defend time you need an anchor outside your own system, a fixed point you cannot move even if you wanted to, so that the existence of a record at a given moment becomes a public fact rather than your private claim. For that anchor we use Pantheon, our sovereign Bitcoin-anchored Layer 1.

### What anchoring actually buys

Anchoring means committing a compact cryptographic summary of a record, or a batch of records, into a public ledger whose history is computationally impractical to rewrite. Once that commitment is settled, the record's existence at that point in time is fixed against a chain that no single party controls, including me. If I later tried to backdate, alter or quietly delete a record, the public anchor would not match, and the discrepancy would be visible to anyone who looked. Anchoring converts who made this and what it said into a far stronger statement: this exact record demonstrably existed by this time, and here is the public chain that proves it.

The phrase Bitcoin-anchored is doing specific work and I choose it carefully. Bitcoin's chain represents the largest and most battle-tested accumulation of irreversible proof-of-work that exists, which makes it the most credible neutral clock available for anchoring. Pantheon is our own sovereign Layer 1, built so the system is self-governing and not at the mercy of someone else's platform, but it borrows the deepest immutability available by anchoring into Bitcoin underneath. The result is a record sealed with post-quantum cryptography on the maker's own hardware, then anchored to a public chain that no authority can rewrite, which is about as close to a tamper-proof historical fact as a digital object can

get.

Stand the three layers together and you see the whole architecture of belief. The signature answers who and what. The standard, FIPS 204, ensures the signature will hold against the computers of tomorrow. The anchor answers when, and removes me, the issuer, from the chain of trust entirely. No layer asks anyone to trust Mickai. Each replaces institutional faith with something checkable, the maths of the signature, the openness of the standard, the immutability of the public anchor. That, in full, is how a genuine artefact comes to carry its own sealed, anchored, independently verifiable proof of what it is.

PART IV · THE STANDARD

# From a record to a right: what changes when proof becomes the norm.

## 10. The Right to Be Believed

All of this machinery exists to deliver one human thing, and it is worth naming bluntly. The right to be believed is the entitlement of an honest person to have their genuine work accepted as genuine, on their own evidence, without depending on the goodwill of a platform or the verdict of a detector. In a world where fabrication is free, this right does not survive on its own. It has to be manufactured, deliberately, with cryptography, because the old social default that used to carry it has collapsed and is not coming back. The provenance record is how the right is manufactured and made durable.

Notice how completely this reverses the burden, and reverses it in the right direction. Under detection, the honest creator is presumed suspect until some classifier clears them, and the classifier can be wrong, gamed or simply absent. Under proof, the honest creator carries their own sealed, anchored record and clears themselves, on demand, to anyone, forever. The burden moves off the genuine and onto the forger, where it belongs, because forging a valid Open Audit Record means forging a post-quantum signature and a public anchor, which is not a matter of a better model but of breaking standardised mathematics and rewriting a public chain.

> **The right to be believed is not granted by a platform. It is earned by a record, and once earned it cannot be taken away.**

This is also the answer to the liar's dividend, the way cheap fakery lets the guilty dismiss real evidence as probable fabrication. When genuine work routinely carries proof, the absence of proof becomes the conspicuous thing. The honest carry their record as a matter of course, so the one who cannot produce one, or whose seal does not verify, stands out. We do not eliminate lying. We make honesty legible and we make its absence visible, and over time that shifts the default back, not to blind trust, but to something better, checkable trust that does not depend on anyone's authority.

The Mickai pantheon.

## 11. What Has to Be True for This to Work

I am wary of architectures that only work in slide decks, so I want to state plainly what conditions must hold for a provenance standard to deliver in the real world, including where the honest answer is not yet. The technical core is the settled part. Signing at creation, sealing with a standardised post-quantum signature, and anchoring to a public chain are all things we have built and can demonstrate. The cryptography is not speculative. ML-DSA-65 is a published standard, and the sealing and anchoring run. That is the ground I am sure of and will defend without caveat.

### Adoption is the hard half

The harder half is adoption, and pretending otherwise would be dishonest. A provenance standard delivers its full value only when creation tools widely capture provenance at the source, and when the surfaces where media is consumed, the feeds, the browsers, the editorial systems, actually surface and check the record. A record no one looks at protects no one. This is why the format must be open and aligned with the wider content-provenance ecosystem rather than a private dialect, because a standard that only one company can read is a feature, not a standard, and features do not change the world.

There are honest limits I will not paper over. Provenance proves origin and integrity. It does not, by itself, prove that what a genuine artefact depicts is true, because someone can authentically film a staged event, and the record will faithfully say it was genuinely filmed. Provenance also cannot retroactively protect the vast existing archive of unsigned media, made before any of this existed. And provenance is not a single switch I can throw alone. It is a standard, which by definition needs others, tool makers, platforms, institutions, to adopt it before it reaches full strength. I would rather tell you that now than oversell a finished revolution.

So I hold two things at once, and I think both are true. The mechanism is real, built, and standing on standardised cryptography rather than on my promises. The standard is a work in progress that depends on adoption I cannot command. Saying both is the only honest position, and it is also the more persuasive one, because the part that is hard is hard for everyone, which is precisely why the part that is solved is worth building on now rather than waiting for a perfect moment that will not arrive.

## 12. Building the Standard, Not Just the Tool

I did not build the Sovereign Intelligence Operating System to win a detection contest. I built it to make a different bet, that the future belongs to provable creation rather than to ever-better forgery spotting, and that the institution which matters is not the best detector but the agreed standard for carrying proof. A tool serves its owner. A standard serves an ecosystem. The Open Audit Record, sealed under FIPS 204 and anchored through Pantheon, is offered as a contribution toward a standard, not as a private moat, because a moat around provenance would defeat the entire point of provenance.

For this to become a standard rather than a feature, the verification side has to be as open as the cryptography. Anyone must be able to take an artefact and its Open Audit Record, check the hash, validate the post-quantum signature against a public key, and confirm the anchor against the public chain, using software they trust rather than software I supply. The day a journalist, a court or an ordinary person can verify one of these records without asking Mickai's permission or running Mickai's code is the day it stops being our product and starts being everyone's standard, and that is the day I am working toward.

> **A standard you cannot verify without its author is not a standard. It is a dependency, and dependencies are the thing we are trying to escape.**

So I will end where I began, with the inversion that makes all of this cohere. Stop trying to spot the fakes and start proving the genuine. Capture provenance at the point of creation, where it can be told truthfully. Seal it on the maker's own hardware with cryptography that will outlive the present generation of machines. Anchor it to a public chain so that no authority, including me, can rewrite history. Then hand the power of verification to everyone. Do those things and you have not merely defended against deepfakes. You have rebuilt, deliberately and verifiably, the thing whose quiet collapse started all of this: the right of an honest person to be believed.

The provenance standard is not a wall against an infinite tide of fakes, because no such wall can be built. It is a passport for the genuine that the tide cannot forge, issued at creation, owned by the maker, sealed against the future and anchored beyond anyone's reach. That is the record that earns the right to be believed. Build it into your tools, demand it of the surfaces you read, and carry it on your own work. The fakes are free and they are not going away. So let the genuine carry proof, and let the proof speak for itself.

The Mickai pantheon.

APPENDIX · ABOUT THE AUTHOR

# Micky Irons

Founder and chief executive of Mickai LTD (Companies House 17166618, registered office 20 Wenlock Road, London, N1 7GU) and named inventor on the Mickai SIOS patent corpus: 101 filed UK patent applications, around 2,234 claims. Trade mark Mickai registered at UK00004373277.

## Profiles

mickai.co.uk

crunchbase.com/person/micky-irons

linkedin.com/in/mickyirons



## References and further reading

· National Institute of Standards and Technology, FIPS 204: Module-Lattice-Based Digital Signature Standard (ML-DSA), U.S. Department of Commerce, August 2024.

· Coalition for Content Provenance and Authenticity (C2PA), Technical Specification for Content Credentials, c2pa.org, 2024.

· Chesney, R. and Citron, D., Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, California Law Review, Vol. 107, 2019, source of the liar's dividend analysis.

· National Institute of Standards and Technology, Post-Quantum Cryptography Standardization Project final reports, NIST, 2022 to 2024.

· Nakamoto, S., Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, foundational reference for proof-of-work anchoring and immutable public ledgers.

· Paris, B. and Donovan, J., Deepfakes and Cheap Fakes: The Manipulation of Audio and Visual Evidence, Data & Society Research Institute, 2019.