

MY WEIRD PROMPTS

Podcast Transcript

EPISODE #340

Carving Bits in Stone: The Power of WORM Technology

Published January 29, 2026 • Runtime: 20:50

<https://myweirdprompts.com/episode/worm-technology-immutable-data/>

EPISODE SYNOPSIS

In this episode, Herman and Corn explore the critical role of WORM (Write Once, Read Many) technology in a digital landscape increasingly defined by generative AI and sophisticated cyber threats. They delve into how hardware-level locks on SD cards and cloud-based compliance modes are becoming the "digital ceremony" of the immutable record, ensuring that once data is written, it can never be altered or deleted. From protecting forensic evidence in criminal investigations to securing "Golden Datasets" for AI training, this discussion highlights why the ability to prevent change is becoming our most valuable asset in 2026. Discover how industries like finance and healthcare rely on these unalterable anchors to maintain trust, meet strict regulatory requirements, and survive the rising tide of ransomware.

DANIEL'S PROMPT

Daniel

We've previously covered digital forensics and the importance of the chain of custody. I'd like to discuss the utility and use cases for WORM (Write Once, Read Many) technology, which ensures that digital evidence remains immutable and tamper-proof. WORM storage is available across various media, from USB drives and SD cards to SSDs and cloud storage like S3 buckets. Beyond legal evidence, it is also highly relevant for financial auditing and medical records. Who is currently utilizing this technology, and how do we verify that it is truly tamper-proof? Let's explore the future of WORM storage in 2026.

TRANSCRIPT

Corn

Hey Herman, welcome back to the table. It is another beautiful day here in Jerusalem, though I think the winter chill of early twenty twenty-six is finally starting to creep through the stone walls of the house.

Herman

It certainly is, Corn. Herman Poppleberry here, and I have actually been wearing two pairs of socks all morning just to keep my hooves warm while I was reading through the latest research papers. But honestly, the prompt Daniel sent us this morning warmed me right up. It is right in my wheelhouse.

Corn

I saw that. Daniel was asking about W-O-R-M technology. You know, it is funny, because I usually think of a worm as something that slowly wiggles through the garden, but in the world of data, it is actually about speed and permanence. Or rather, the lack of change. Write Once, Read Many.

Herman

Exactly. And it is such a fascinating contradiction in our modern digital world. We spend so much time talking about how data is fluid, how it is constantly updated, synced, and versioned. But W-O-R-M technology is the exact opposite. It is the digital equivalent of carving something in stone. Once those bits are set, they are essentially unchangeable.

Corn

It feels almost rebellious in twenty twenty-six, doesn't it? In an era where we can use generative artificial intelligence to alter photos, videos, and even historical records in seconds, having a technology that says, no, this is exactly what happened and it can never be changed, feels more important than ever.

Herman

You hit the nail on the head. That is precisely why the utility of W-O-R-M has exploded recently. Daniel mentioned digital forensics and the chain of custody, which we have touched on in previous episodes, but the scope of this is just massive now. It is the backbone of trust in a world where trust is becoming a very rare commodity.

Corn

So, let's start with the basics for a second, because I think people might confuse this with just a read-only file. If I right-click a file on my computer and select read-only, that is not W-O-R-M, right?

Herman

Not even close, Corn. A read-only attribute in an operating system is like a polite sign that says, please do not touch. But anyone with administrative privileges can just ignore the sign and change the file anyway. True W-O-R-M technology happens at the hardware or the deep system level. It means the physical ability to overwrite that specific sector of the storage medium is either physically destroyed or cryptographically locked away by the controller itself.

Corn

I remember when we talked about optical media back in episode three hundred and eight. We were discussing how a laser actually burns a physical pit into the surface of a C-D-R or a D-V-D-R. That is the classic example, right? Once the pit is burned, you can't un-burn it.

Herman

That is the gold standard of hardware W-O-R-M. It is a physical change to the material. But as Daniel pointed out, we have moved way beyond shiny silver discs. Today, we are seeing W-O-R-M implemented in S-D cards, solid state drives, and even in the cloud. Companies like Swissbit are leading the way here, creating industrial-grade S-D cards where the firmware itself acts as a gatekeeper.

Corn

That is the part that gets me. How do you do that with a flash drive or an S-D card? Because there is no laser involved there. It is all just electrical charges in silicon.

Herman

It is really clever. In a W-O-R-M-enabled S-D card or U-S-B drive, the controller inside the device is programmed at the factory. When a block of data is written, the controller essentially blows a virtual fuse for that block. It marks that sector as permanently closed to new writes. Even if you take that card and put it in a different computer, the hardware itself will refuse any command to modify that data. It will return an error every single time.

Corn

So it is like a one-way gate. But I imagine that creates some interesting challenges for the people actually using it. If you make a mistake while writing the data, is that it? Is the drive just ruined?

Herman

Pretty much. That is why the software that handles the writing process has to be incredibly robust. You usually have a staging area where you verify everything, calculate your hashes, and then you commit it to the W-O-R-M media. It is a very deliberate act. It is not like saving a Word document where you hit control-S every five minutes. It is more like a digital ceremony.

Corn

I love that image. The Digital Ceremony of the Immutable Record. But let's talk about why we need this ceremony. Daniel mentioned legal evidence and the chain of custody. If I am a forensic investigator in twenty twenty-six, how am I using this?

Herman

Imagine you are at a crime scene. You find a laptop or a phone. You need to make a bit-for-bit copy of that drive, what we call a forensic image. Now, if you save that image to a regular hard drive, a defense attorney could argue in court that you, or someone else with access to that drive, could have opened the file and changed a few bytes to plant evidence.

Corn

Right, and even if you didn't do it, just the possibility that you could have done it creates reasonable doubt.

Herman

Exactly. But if you write that forensic image directly to W-O-R-M media, and you can prove the media was W-O-R-M-compliant from the moment it left the factory, that argument disappears. The technology itself becomes the witness. It says, it was physically impossible for this investigator to change this data after it was written.

Corn

That makes total sense for police work, but Daniel also brought up financial auditing and medical records. Those seem like areas where things are constantly changing. If I go to the doctor, they add new notes every time. How does W-O-R-M work in a living document?

Herman

That is where we get into the difference between the record and the system. In healthcare, under regulations like H-I-P-A-A in the United States, you need an audit trail. You might update a patient's chart, but the original entry from three years ago must remain intact and unalterable. You don't overwrite the old data; you write a new version. In a W-O-R-M-based system, every single version is saved to an immutable bucket.

Corn

So it is like a stack of papers where you can only add a new page to the top, but you can never erase or white-out anything on the pages underneath.

Herman

Precisely. And in finance, it is even more strict. The Securities and Exchange Commission, the S-E-C, has Rule seventeen a-four. While they recently added an audit-trail alternative, many firms still stick to W-O-R-M because it is the most ironclad way to prevent companies from cooking the books after the fact. If a regulator comes knocking, they want to see the raw, original data, not a version that was polished three weeks later.

Corn

I'm curious about the cloud side of this. Daniel mentioned S-three buckets. For those who don't know, that is Amazon's Simple Storage Service, which is basically the giant hard drive of the internet. How do you have a W-O-R-M drive in the cloud? There is no physical fuse you can blow in a data center thousands of miles away.

Herman

This is where we move from hardware W-O-R-M to software-defined W-O-R-M, or what is often called Object Lock. But here is the critical distinction for twenty twenty-six: you have to choose between Governance mode and Compliance mode. In Governance mode, users with special permissions can still delete the data. It is like a locked door where the manager has the key.

Corn

And Compliance mode?

Herman

Compliance mode is the vault with the key thrown into the sun. Once you set a retention period in Compliance mode, even the root user, the person with the highest level of authority at your company, cannot delete that data until the timer expires. Not even Amazon support can delete it for you. It is a programmatic lock that is enforced by the very architecture of the cloud service.

Corn

That sounds incredibly powerful, but also a little scary. If I accidentally upload ten terabytes of cat videos and set a ten-year W-O-R-M lock on them, I am paying for that storage for the next decade, no matter what?

Herman

You are indeed, Corn. You would have the most legally-defensible collection of cat videos in history, and a very consistent monthly bill to match. It is a high-stakes game. But for a corporation facing a multi-billion dollar lawsuit, that cost is a drop in the bucket compared to the risk of being accused of destroying evidence.

Corn

We have talked about the who and the why, but I want to dig into the verification part of Daniel's prompt. Because if I am a judge, or a regulator, I am not just going to take your word for it that your S-D card is tamper-proof. How do we actually verify this in twenty twenty-six?

Herman

This is the critical question. Verification usually happens in three layers. The first is the physical or hardware certification. You have independent labs that test these devices. They try to hack the controllers, they try to bypass the fuses with high voltage, they try everything to see if they can force a write. If the device passes, it gets a certification, like F-I-P-S one hundred and forty dash three, which is the current gold standard for cryptographic modules.

Corn

Okay, so Layer One is trust in the manufacturer and the testing labs. What is Layer Two?

Herman

Layer Two is cryptographic. Every time you write a piece of data to W-O-R-M media, you generate a hash, which is like a digital fingerprint. We talked about this a bit in the subsea fiber episode, episode three hundred and thirty. If even a single bit of that data changes, the hash will look completely different. By recording that hash at the moment of creation and then checking it later, you can prove the data is identical.

Corn

But couldn't someone just change the data and then generate a new hash to match the new, fake data?

Herman

Not if the hash itself is stored on W-O-R-M media or in a public ledger. This is where some people are using blockchain technology as a timestamping service. If you take the hash of your forensic image and you publish it to a source that everyone can see and that no one can change, you have created a permanent anchor.

Corn

And what is the third layer?

Herman

The third layer is the firmware level. Many modern W-O-R-M devices use something called signed firmware. The device will only run code that has been digitally signed by the manufacturer. This prevents a hacker from loading a custom operating system onto the S-D card that would allow them to bypass the write-protection. It is defense-in-depth.

Corn

It is like having a safe that is inside a vault, and the vault is at the bottom of the ocean. Which brings us to the future of W-O-R-M. Why is this so relevant right now, in January of twenty twenty-six?

Herman

Two words,

Corn

Ransomware and A-I. We have seen ransomware attacks get so sophisticated in twenty twenty-five. They don't just encrypt your files anymore; they go after your backups first. They find your backup server, they delete everything, and then they encrypt your main system so you have no choice but to pay. W-O-R-M is the only thing that stops that delete command.

Corn

And what about A-I? How does W-O-R-M help there?

Herman

This is the big trend for twenty twenty-six: Data Provenance. We are seeing these massive lawsuits about A-I models being poisoned by bad data or infringing on copyrights. If you are building a model, you need a Golden Dataset—a human-generated ground truth that you can prove hasn't been tampered with by an adversary or another A-I. Storing your training data on W-O-R-M media ensures that your A-I's education is verifiable and clean.

Corn

It is about creating a ground truth. In a world of deepfakes and hallucinating A-I's, we need a way to point to something and say, this is the original, unadulterated reality.

Herman

It is funny, isn't it? We spent decades trying to make storage faster, smaller, and more rewritable. And now, the most valuable feature we can offer is the inability to change. It is a total reversal of the digital trend.

Corn

It reminds me of that old saying that the more things change, the more they stay the same. Except in this case, the more things change, the more we need them to stay exactly the same. So, Herman, for someone listening who wants to use this, how accessible is it?

Herman

It is actually becoming surprisingly accessible. You can buy W-O-R-M-enabled S-D cards from industrial suppliers like Swissbit right now. They are more expensive, obviously, because you are paying for that specialized controller and the F-I-P-S certification. For the average person, it might be useful for things like a digital will, or preserving family photos that you never want to accidentally delete.

Corn

But you have to be careful. W-O-R-M is a commitment. If you put your photos on a W-O-R-M drive and then you realize you want to crop one of them, you can't save the changes back to that drive. You have to start over on a new piece of media.

Herman

It really forces you to be intentional. I think that is a good thing. We live in such a disposable digital culture. W-O-R-M is the digital equivalent of film photography. You have a limited number of shots, and they are permanent. I think there is a real psychological value in that.

Corn

So, looking ahead through the rest of twenty twenty-six, where do you see this going? Do you think W-O-R-M will eventually become the default for certain types of data?

Herman

I think we are going to see it integrated into the hardware of our devices more deeply. Imagine a smartphone where the core operating system files are stored on a W-O-R-M partition at the factory. It would make it virtually impossible for malware to get a persistent foothold in the system, because the malware literally could not write itself into the boot sequence. It would basically end the era of the rootkit.

Corn

That would be a massive leap for security. It feels like we are finally pouring concrete into the sand that the internet was built on. Herman, this has been a blast. I always learn something new when we dive into these technical rabbit holes.

Herman

Same here, Corn. And thanks to Daniel for the prompt. It kept my brain busy enough to forget about my cold hooves for at least twenty minutes.

Corn

Well, we should probably get some more wood for the fire then. To everyone listening, we really appreciate you spending your time with us. If you have been enjoying My Weird Prompts, please take a second to leave us a review on Spotify or wherever you get your podcasts. It genuinely helps other curious people find the show.

Herman

It really does. And you can always find us at our website, myweirdprompts.com. We have the full archive there, and a contact form if you want to send us a prompt of your own. Maybe your idea will be the focus of episode three hundred and thirty-six!

Corn

We would love to hear from you. Until next time, keep asking the weird questions.

Herman

Goodbye from Jerusalem!

Corn

So Herman, about those two pairs of socks... are they W-O-R-M-compliant?

Herman

They are definitely write-once, because once I put them on, I am not taking them off until the spring!

Corn

Fair enough. Let's go find that wood.

Herman

Lead the way, Corn. Lead the way.