

Police Force Management System (PFMS)

Securing the entire chain of evidence: Pre-Crime Evidence, Crime Investigation (FMS), Evidence Storage Facility, Prosecution, and Court of Law.

TREASURY ASK

₹9,600,000

over 15 months

ON CHAIN VOLUME

**1.5 Million+
Transactions a Year**from year one, and rising every year
after

FIRST USER

**Indian State
Government**

PROPOSAL BY

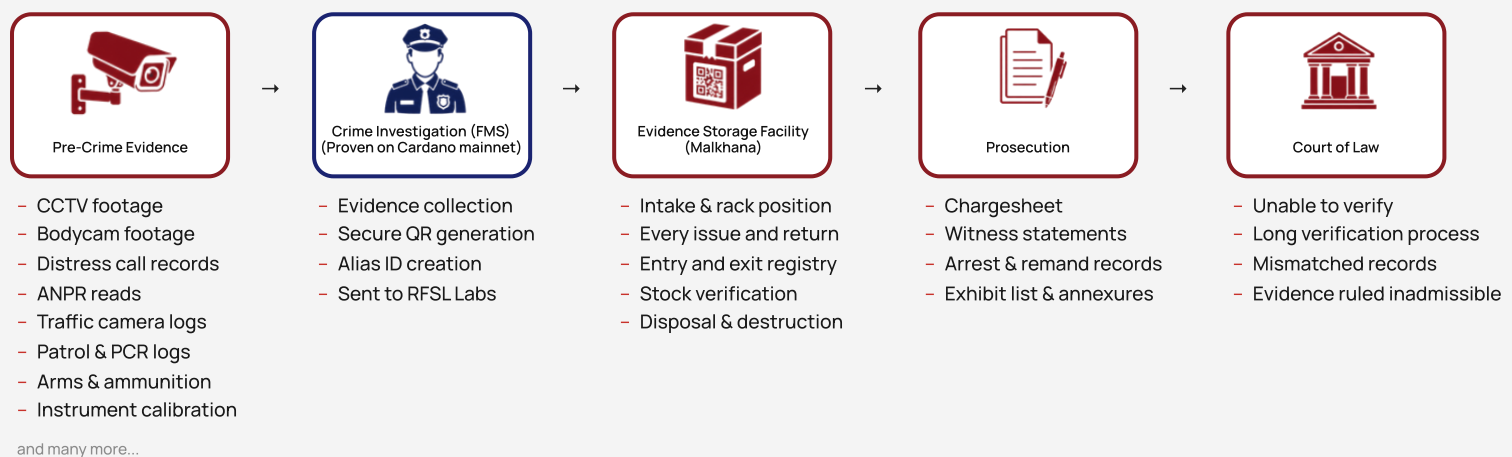
Trivolve Tech

Police Force Management System (PFMS)

Problem

The entire chain of evidence is divided into 5 stages: Pre-Crime Evidence, Crime Investigation (FMS), Evidence Storage Facility, Prosecution, and Court of Law. FMS, one of the PFMS components, is proven on Cardano mainnet and secures one of these five stages. The other four remain vulnerable to fabrication. This is not a problem confined to one state or one country. Justice systems around the world face it.

When the integrity of any of these 5 stages is compromised, the consequences go far beyond a failed case. They can mean an innocent person losing their freedom, a victim being denied justice, and a life being permanently destroyed. It also takes time. A case in Telangana takes an average of 7.5+ years to resolve, much of it spent arguing over whether the records can be trusted rather than over what happened.



How are we Solving this?

Our **open source** solution, PFMS, secures the entire chain of evidence by recording and stamping every critical action on **Cardano** across all five stages: Pre-Crime Evidence, Crime investigation (FMS), Evidence Storage Facility, Prosecution, and Court of Law. This makes not just the chain of custody but the entire chain of evidence tamper evident. PFMS is built once as an open source core and rolled out to multiple states, starting with Telangana.

PFMS does not just protect evidence. It also protects the truth behind every case, helping make it far harder for the guilty to escape through altered evidence, or for the innocent to be convicted on it. Also, every record can now be verified against Cardano in moments. **This alone will cut the time taken to solve a case by around 30 percent.**



**From the first piece of evidence, even before the crime, to the final verdict,
no record can be altered or removed afterwards without it showing.
Every step in the chain of evidence is permanently stamped on Cardano.**



Contents

I	Problem	4
	Breaking Down Each Stage · Pre-Crime Evidence · Crime Investigation · Evidence Storage · Prosecution · Court of Law	
II	Solution	12
	What We Are Doing · The Five Stages · Pre-Crime Evidence · Crime Investigation (FMS) · Evidence Storage · Prosecution · Court of Law · What Changes	
III	Technical	20
	The Problem and How PFMS Answers It · Evidence Stack · Journey of the Records	
IV	Ecosystem Fit	23
	Why Cardano · Already Running Chain of Custody · Impact · What It Means for Cardano · Revenue Potential Beyond Transactions · Cardano 2030 KPI Alignment	
V	Team and Track Record	33
	Trivolve Tech · Quixy · A Team Built for This Scale · Who Owns PFMS	
VI	Funding Ask	37
	The Ask · Disbursement Schedule · Budget Allocation · Work Packages · Milestones and Acceptance	
VII	Governance and Withdrawal Management	48
	Constitutional Compliance · Withdrawal Guardrails · Administration	
VIII	Risk Management	50
	Build Failure · Data Feeds · Adoption · Financial Discipline	
IX	Conclusion	52
	What It Opens · What It Comes To	



1. Problem

A criminal case is built on evidence. That evidence does not sit in one place and it does not stay with one person. It starts with a camera or a phone call even before a crime is reported then passes through the hands of police officers. It then sits in a storeroom for years, gets copied into court documents, and finally reaches a judge.

At almost every one of those points a record is made, and most of those records exist. What none of them can show is that they have not been altered since, or that they were made when they say they were.

Think about what happens in a courtroom. A defence lawyer stands up and says the CCTV footage was erased after the case was registered (in India, the First Information Report, or FIR). Or that the calibration certificate for the breathalyser was created later and back dated. Or that pages of the evidence storage facility register (the Malkhana register, in India) were rewritten before the exhibit was produced.

The lawyer does not have to prove any of it. Raising a reasonable doubt is enough. Once that doubt is on the record, it is the prosecution that has to show the evidence is exactly what it claims to be.

And this is where the case falls apart. The police can produce the register. They can produce the footage. What they cannot produce is anything that proves the register was never rewritten, or that the footage is complete and unedited. The record and the claim about the record come from the same place, so the record cannot be used to verify itself.

So the case stops turning on what happened and starts turning on what cannot be ruled out. Evidence gets ruled inadmissible. Investigations that were done correctly collapse anyway. And none of this depends on whether tampering actually took place, because the police have no way to demonstrate either way.

That is the problem we are solving: strengthening the chain of evidence so that honest police work is backed by a verifiable record of how evidence was captured, handled and preserved, from its source to the courtroom.

This is not a problem confined to one state or one country. Wherever the department that creates a record is also the only one that keeps it, the same gap exists, and justice systems around the world face it.

The full journey of evidence runs through five stages. Our earlier system, FMS, secures one of them. The other four are still open.

The five stages

#	STAGE	WHAT HAPPENS HERE	WHAT THE DEFENCE CAN ALLEGE	WHY THE POLICE CANNOT DISPROVE IT TODAY
1	Pre-Crime Evidence	Cameras, call logs, sensors and equipment records that already exist before any crime is reported	The footage was trimmed or erased after the crime. The calibration certificate was back dated	Nobody recorded what the footage originally contained. There is no earlier version to compare against
2	Crime Investigation (FMS)	Officer collects evidence from the scene, seals it, labels it, sends it to the forensic lab	Already secured by FMS	Proven on Cardano Mainnet, and every action here carries a stamp the police can point to. Specific modules are yet to be built for this state
3	Evidence Storage (Malkhana)	Physical evidence is stored, issued to court or lab, returned, verified, and eventually destroyed	The register was rewritten. The exhibit was swapped or handled off the record	The register is the only account of itself. Producing it proves nothing about whether it was altered
4	Prosecution	Chargesheet, witness statements, arrest records and exhibit lists are prepared for court	The exhibit list was changed. An annexure was added or removed after filing	Court documents are written by hand, not generated from the underlying record. No fixed version exists to check against
5	Court of Law	Judge checks where evidence came from, whether it is authentic, and whether it can be used	All of the above, raised together	The court is asked to rely on certificates and testimony from an interested party.

WHAT IT COSTS WHEN ANY OF THESE STAGES FAIL

The visible cost is years lost in court.
The real cost is justice or verdict itself.

When authentic evidence cannot be proven authentic, the guilty can walk free. When fabricated evidence cannot be exposed, the innocent can lose their freedom.



1.1 Breaking down each stage

Below we go through each of the five stages one at a time. For each stage we explain what evidence lives there, how it is handled today, and exactly where it can be tampered with.

STAGE ONE

1.1.1 Pre-Crime Evidence

WHAT THIS STAGE IS, IN PLAIN TERMS

This is all the evidence that already exists before anybody knows a crime has happened.

A street camera recording the street. A police bodycam that was already running. A call to the control room. A number plate reader on a highway. A logbook of which patrol vehicle was where. A register of which weapon was issued to which officer. A certificate saying a breathalyser was calibrated last month.

None of this was created for the case. It was already there. Then a crime happens, and suddenly it becomes the most important material in the investigation.

These are working systems, not evidence systems.

The control room log, the patrol and PCR log, the armoury register and the calibration file all exist to run day to day policing. They were never designed to be held up in a courtroom years later.

That means they behave the way working systems behave. Entries get corrected when someone notices a mistake. A log is written up at the end of a shift rather than in the moment. A register is rewritten when the old one is full. Storage gets rotated and consolidated. Every one of these is normal, legitimate, and happens constantly.

The problem is that the system keeps only the current version. It does not keep a record of what changed, who changed, when, or why. So a routine end of shift correction to a patrol log and a deliberate alteration to that same log leave behind exactly the same thing: one entry, no history. The police cannot tell the difference after the fact, and neither can the court. The defence does not need to prove anything happened. It only needs to point out that nobody can show it did not.

What is recorded at this stage

The list below covers the main categories of Pre-Crime record at this stage. Every one of them is made by the department that later has to defend it.

1. CCTV and Bodycam footage

Cameras at streets, police stations, checkpoints and lock-ups.

HOW IT IS MADE The camera records over its old footage again and again. It becomes a file only when someone opens the timeline, picks a start and end time, and saves that piece.

WHERE IT CAN BE CHANGED At the export step. When the court asks for footage, someone has to sit at the recorder and pull it out. Only the part they select comes out. The rest stays behind and is written over soon after.



So a person can export one part, leave the rest out, and say the camera was not working for those minutes. Or the camera really was not working for those minutes. Afterwards the two look exactly the same.

WHAT IT COSTS A man dies in custody of natural causes. The station says the camera was faulty that night and produces no footage. The defence says the camera was working fine and the police removed the part that mattered.

Both stories end at the same place. No footage.

Today nothing separates them. A camera that was dead leaves nothing behind. A recording that was cut out also leaves nothing behind. The department has no way to prove which one happened.

2. Distress call records

Emergency calls, and the entry made about them.

HOW IT IS MADE A call comes in. The control room records the call along with the time it arrived, and then dispatches a police van to the location.

WHERE IT CAN BE CHANGED All of it sits in the control room's own records. The recording and the time entry are both held in the same place, by the same people.

If the recording is missing, it could be a technical fault. Or it could have been there and been removed later. If the time entry says one thing, it could have said that from the start, or it could have been changed afterwards. Neither can be proven.

WHAT IT COSTS A woman calls for help at night. Police reach an hour later and by then she is dead. Her family says she called at 9:14. The control room record shows the call at 9:50 and the unit reaching at 10:05.

Both stories end at the same place. One entry in the system, saying 9:50.

Today nothing separates them. The department has no way to prove which one happened.

3. ANPR (Automatic Number Plate Recognition)

Number plate cameras on highways, toll points and checkpoints.

HOW IT IS MADE A camera takes a photo, software reads the plate, and the plate, place and time go into a database on their own.

WHERE IT CAN BE CHANGED After the entry is saved. It sits in a database that can be edited. The system does keep logs of what was added, corrected, deleted or changed, but those logs themselves are editable.

WHAT IT COSTS One entry says a car, and the person in it, was at a place at a time. In court that looks solid, because a machine made it and no person touched it.

But it sits in a database, and a database can be edited. A defence lawyer only has to say so. There is no answer to it.

4. Patrol logs and the station diary

The most used record in any police station.

HOW IT IS MADE Everything that happens at a police station goes into one record. Who came in, who was arrested, which van went where, at what time. It is entered digitally, by the duty officer, as the day goes on.

WHERE IT CAN BE CHANGED After the entry is made. An entry can be edited or removed later by anyone with the right access, and the record of that edit sits in the same system, under the same access.

What reaches a court is an extract from that system.



WHAT IT COSTS A man is picked up on a Friday evening and produced before a magistrate on Sunday afternoon. He says he was in the lock-up from Friday. The station says he was arrested Sunday morning.

The whole question is one entry in the station record, and what is filed in court shows Sunday morning.

Today nothing separates them. A station where the arrest really happened Sunday has a Sunday entry. A station where a Friday entry was made and later removed also has a Sunday entry and nothing else. The department has no way to prove which one happened.

5. Arms and ammunition records

Every police station and armed battalion has a locked armoury, called the Kot in India. All weapons and ammunition live there, and one officer, the armoury officer (the Kot officer), is answerable for everything inside it.

HOW IT IS MADE Two records run the room.

The first is the stock register. It lists everything the station holds, by make, calibre and serial number, so at any moment there is a stated figure for what should be in the room.

The second is the issue register. Every time a weapon leaves the Kot, an entry is made with the officer's name, his batch number, the exact time he took it, and his signature. Another entry is made when he brings it back.

WHERE IT CAN BE CHANGED At the entry. Nothing records when an entry was actually written, so a line can be filled in on any day carrying any time.

Weapons are tracked by serial number. Individual rounds are generally accounted for by quantity, type and batch. That makes the issue and return records particularly important. If those records are altered, establishing how many rounds were issued, returned or reported as fired becomes harder.

WHAT IT COSTS An officer takes his weapon and ten rounds from the Kot in the evening. That night there was a firing. He says he fired two rounds. A man is dead and the family says far more than two shots were fired.

The register is the only place that can settle it. The software puts the time on the entry by itself, so nobody had to write it. It shows ten rounds issued in the evening and eight returned.

But the entry is still a row in a system, and a row in a system can be edited. The time it carries can be edited with it and can be questioned in court with no way for the police department to prove otherwise.

6. Instrument calibration records

Certificates showing that breathalysers, speed guns and weighing scales were working.

HOW IT IS MADE The instrument is checked against reference standards. A certificate records its identity, the calibration date and the results. A next calibration or verification due date is recorded where applicable.

WHERE IT CAN BE CHANGED If a certificate is altered, replaced or falsely backdated, establishing its history depends on the issuing laboratory's records and the department's retained copies. Where those records are incomplete or difficult to reconcile, confirming which version existed before a disputed reading becomes harder.

WHAT IT COSTS Missing or inconsistent calibration records can make it harder to demonstrate that an instrument's reading was reliable when it was taken. Investigators may need additional laboratory records or expert evidence to resolve the uncertainty.



STAGE TWO

1.1.2 Crime Investigation (Proven on Cardano Mainnet by FMS)

WHAT THIS STAGE IS, IN PLAIN TERMS

A crime is reported. The forensic team reaches the location and collects the evidence: blood, weapons, soil, fingerprints. Back at the station the case is registered and a Case ID is generated. That Case ID is pasted on every evidence box. The boxes are then sent out to multiple forensic laboratories for testing, one for blood, one for bone, one for fingerprints, and so on.

Unlike every other stage, the evidence here does not sit still. It moves. And it moves with its own name written on the outside.

What the problems were

Everything at the scene was recorded by hand.

The team collected the evidence and wrote it down manually. Paper tags, a notebook, photos on whatever camera they were carrying. At that moment the evidence existed but had no identity that anything could trace back.

The Case ID came later, and it was in plain text.

The number is generated at the station, after the evidence has already been collected and packed. It is then printed and pasted on every box, readable by anyone who walks past.

And the number is not random. 61/2024/05/65/22042 spells out the police station, the year, the month, the case number and a time stamp. Anyone who sees a box learns which case it belongs to and where it came from.

The boxes then travelled, wearing that number.

The evidence goes out to multiple laboratories. Different buildings, different staff, several handovers, each one signed on paper. A signature proves that a person signed. It does not prove that the box they signed for is the box that reached the other end.

How it came apart

A person working from outside did not need much. The box told them which case it belonged to. Once they knew that, they could follow it, and they could reach it at more than one point on the way.

And they did not even have to succeed. Once the chain of custody is questioned in court, a small gap is enough for the whole evidence to be thrown out. Destroying the evidence was never necessary. Making it impossible to prove the evidence was clean did the same job.

This stage is now proven on [Cardano mainnet](#) by FMS, with over **156,000 transactions** stamped.



STAGE THREE

1.1.3 Evidence Storage Facility (Malkhana)

WHAT THIS STAGE IS, IN PLAIN TERMS

The Malkhana is the storeroom where seized evidence lives. A weapon, a phone, a bloodstained shirt. It comes in, it is given a rack, and it stays there. It is taken out when a court or a laboratory asks for it, and it comes back again afterwards. It stays this way until the case ends, which can take five years, or ten. This is the longest any evidence sits anywhere in the chain, and for that whole time one register in one room is the only account of what happened to it.

The problems, one by one

WHAT HAPPENS	HOW IT IS HANDLED TODAY	WHAT IT COSTS IF CHANGED OR ALTERED
Intake and rack position	An item arrives and someone writes down what it is and where it has been put. Rack four, shelf two. The item and its place in the room are joined only by that line. Nothing else connects them. If the line says rack four and the item is on rack six, or the item on rack four is not the item the line describes, there is nothing in the room that would show it.	Two similar packets in a case. The register says which is which. Change the line, or move the packets, and the register still reads perfectly. The court receives a sealed packet with a number on it and no way to know if that number belongs to it.
Every issue and return	The exhibit leaves for court or for a laboratory, and comes back. Each time, an entry is made. Over the years of a case this happens again and again. Different officers, different courts, different labs. Each movement is one line, written by whoever was on duty. Nobody outside the room ever sees it happen.	A defence lawyer asks how many times the exhibit left the Malkhana and who had it. The register gives an answer. But the register is the only thing that knows, and it is kept by the same office that had custody. A movement that was never written down did not happen, as far as anyone can tell.
Entry and exit registry	A separate record of who walked into the Malkhana and when. This is the record that answers the question of who had access. It is written at the door, by hand or in a system the station runs.	When an exhibit is found tampered with, this is the first record anyone asks for. It names everyone who was near it. Which is exactly why it is the first record anyone would want changed, and there is nothing to show whether it was.
Stock verification	From time to time, someone checks the room against the register. The check compares what is on the shelves to what the book says should be on the shelves. If the two agree, the room passes.	The check can only find things that are missing. It cannot find things that were swapped, because a swapped item still makes the count come out right. And a shortfall found today has no way of being placed in time. Nobody can say whether the item went missing last week or four years ago, or who was responsible when it did.
Disposal and destruction	When a case ends, the exhibit is destroyed and an entry records that it was. That entry is the last thing anyone will ever see about that item. After it, there is no item left to check anything against.	An entry saying an item was destroyed and an entry saying an item was destroyed while the item was quietly taken away look exactly the same. This is the only step in the entire chain that cannot be reviewed afterwards, because the evidence itself is gone.

STAGE FOUR

1.1.4 Prosecution

WHAT THIS STAGE IS, IN PLAIN TERMS

By now the evidence has been collected, tested and stored. The investigating officer prepares a chargesheet setting out the case, attaches the statements witnesses gave, the records of when the accused was arrested and how long he was held, and a list of every exhibit being relied on. That bundle is what the court reads, and for most of the trial it is what the court works from. The evidence itself sits in a storeroom somewhere. The case in front of the judge is the file.

That is what makes this stage different from every other one. Everywhere else, a record describes something that happened. Here, someone sits down and writes the case out.

Chargesheet

People assume a chargesheet is final once it is filed. It is not.

The law allows it to change, and it changes often. If the police find new evidence or a new accused after filing, they file a supplementary chargesheet. During the trial the court itself can add, alter or drop charges as the evidence comes out. And the High Court can strike out part of it, or all of it, if it finds the allegations do not hold.

All of this is proper. A case that could never be corrected would be a worse system than one that can.

But it means the file the judge reads at the end of a trial is often not the file that was filed at the start. Pages have been added. Sections have changed. Parts have gone.

Now picture the defence saying that a line in the chargesheet about the time of the incident is not what the copy served on them in March said. The prosecution says it always said that.

Both sides point at the same file.

Nothing anywhere shows what the March version said. There is no fixed copy of version one to hold the current one against. A change made through the proper legal route and a page quietly replaced arrive at the same place: one clean document on the record, and no way to see what came before it.

Witness statements

A witness speaks. An officer records what was said. The written statement becomes part of the investigation file.

Months later, the witness stands in court and gives a different account. He says the officer misunderstood him, left something out, or recorded words he never used.

Where no audio or video recording exists, establishing exactly what was said can be difficult. A further question may arise: is the statement in the file the same version originally recorded?

These are separate questions. Preserving the original record cannot prove that it accurately captured the witness's words. But a verifiable history can help establish whether that record was subsequently changed, giving the court a firmer basis for examining the disagreement.

Arrest and remand records

The law is strict here. A person who is arrested must be produced before a magistrate within twenty four hours. Every extension of custody after that has to be recorded too.

These times go into the file by being copied out of the station's own records.



A man says he was picked up on Friday night and kept in the lock-up all weekend. The file says he was arrested on Sunday morning and produced before a magistrate on Sunday afternoon. Five hours. Well inside the limit.

His freedom for those two days rests entirely on which version is true. And both versions are just entries, copied from one record kept by the station into another document written by the station.

The office being asked the question is the office that wrote both answers.

Exhibit list and annexures

The exhibit list names every item the prosecution is relying on. It is typed up from the Malkhana records and filed along with the chargesheet.

That list decides what is in the trial. An item on it is part of the case. An item left off it is not part of the case, no matter what is sitting in the storeroom.

Twelve items were seized. The list carries eleven. The knife is not on it.

Maybe it was never seized. Maybe it was lost somewhere in the Malkhana years ago. Maybe it was left off because it did not help. Nobody in the courtroom can tell, because the list was retyped by hand rather than pulled from the storeroom records, so a mismatch between the two looks the same whether it was a typing slip or a decision.

This is the quietest gap in the whole chain. Nobody has to destroy a piece of evidence. They only have to not type a line.

What all of this adds up to

At this stage the case stops being a set of events and becomes a set of documents. And documents can be written, rewritten, added to and amended, sometimes for very good reasons.

So when a defence lawyer says a page was changed, or a name was added, or a statement was written more strongly than the witness spoke it, there is nothing to compare against. There is only the version on the record, and the officer's word that it is what he always wrote.

The officer who wrote it honestly and the officer who did not both file one clean document, signed and dated. Nothing separates them.

STAGE FIVE

1.1.5 Court of Law

Everything in the four stages before this one arrives here, and the judge has to decide whether to trust it. That is harder than it sounds. The footage, the registers, the statements and the exhibit list all come from the same place, and each one can only be checked against a certificate or an officer's testimony saying it is genuine. So verification turns into a process rather than a moment. Witnesses are called to speak about procedure instead of facts, files go for examination, dates are compared, and hearings stretch across years.

When two records do not agree, and across four stages of hand copied entries they often do not, nobody can say which one is right, only that they differ. And at the end of it the judge is often left with no choice but to keep the evidence out of the case altogether, because evidence that cannot be shown to be what it claims to be cannot safely be relied on to convict anybody. That is where a case dies. Not because the truth came out, but because it could not be established either way.

Somewhere in every one of these cases is a person waiting to find out what happens to the rest of their life. They deserve a verdict built on what actually happened, not on what nobody could prove either way.



2. Solution

2.1 What we are doing, in plain terms

The problem was never that police records are wrong. It was that a record kept by the department cannot prove anything about itself, so a defence lawyer only has to ask a question and the department has no answer.

We are building a unified, modular and open source system for the entire chain of evidence, designed for any police force and justice system, where every point across all five stages is fingerprinted and signed where it is created.

Every point where a record is born. The camera and the recorder. The control room console. The armoury register. The Malkhana shelf, the rack, the issue slip and the destruction order. The chargesheet, the statement, the exhibit list. Some of these are already digital and simply have no way of proving themselves. Some are still paper. All of them come into one system that knows the moment a record comes into existence, takes a digital fingerprint of it, and stamps that fingerprint on Cardano before anyone has had the chance to touch it.

A fingerprint is not a copy. Run any file or entry through a standard calculation and out comes a short line of characters (hash). Change anything, even one second of audio, and that line comes out completely different. It works one way only. The record gives you the fingerprint. The fingerprint gives you nothing back. The fingerprint never travels alone. It is signed together with the device that produced the record and the credential of the officer on duty, so who made it is part of the stamp rather than a note beside it.

No evidence ever leaves the department. No footage, no call recordings, no statements, no names, no case files. Only the fingerprint goes out, and a fingerprint on its own tells a stranger nothing at all.

Years later, when a record is produced in court, it goes to the verification layer. The record is fingerprinted again and read against what Cardano has held since the day it was stamped. If it matches, the record is exactly what it was, and the report says so along with who made it and whether they were authorised at the time. If it does not match, the record has changed. Prosecution, defence and the court each submit the same record and receive the same answer.

There is no third answer, and no opinion involved. What PFMS proves is that a record has not changed since it was made, and who made it. It cannot prove the original entry was truthful. That still rests on the officer and the court, but a false entry can no longer be quietly rewritten later.

Our unified system PFMS does not interfere with how policing is done today. It sits on top of what already exists. The stamping happens in the background, without the officer noticing it at all.

2.2 The five stages

#	STAGE	WHAT THE DEFENCE CAN ALLEGE	WHAT THE POLICE CAN NOW SHOW
1	Pre-Crime Evidence	The footage was trimmed. The certificate was back dated	The record carries a stamp from the day it was made. It either matches or it does not
2	Crime Investigation	Already secured by FMS	Proven on Cardano mainnet, with specific modules for this state yet to be built
3	Evidence Storage (Malkhana)	The register was rewritten. The exhibit was swapped	Every intake, issue, return and check is fingerprinted and signed as it happens
4	Prosecution	The exhibit list was changed. An annexure was added after filing	Every version of every document is stamped. The court can see what version one said
5	Court of Law	All of the above, raised together	The court checks the record itself, instead of taking somebody's word for it

STAGE ONE

2.3 Pre-Crime Evidence



1 CCTV and bodycam footage

Two officers on patrol wear bodycams. Down the street a person is being robbed, and the pole camera above catches it. Both recordings are stamped as they are written, so the footage that reaches court is the footage the cameras saw.

2 Distress call records

In the control room two operators take the call about the robbery and log it. The recording and the entry are stamped as they are made, so crucial details such as the time of the call cannot be argued about later.

3 ANPR

The white car passes under the number plate camera. The plate, the time and the place are captured and stamped at once, so the record of that car being there cannot be added or removed afterwards.

4 Patrol logs and the station diary

At the station desk an officer writes up the incident in the diary. Every entry is stamped the moment it is saved, so what the diary says today is what it said that day.

5 Arms and ammunition records

In the armory an officer issues weapons and logs each one. Each issue and return is stamped at the time, so the register can show exactly who held what and when.

6 Instrument calibration records

At the roadside an officer tests a driver with a breathalyser. The instrument carries a calibration certificate, signed on the day it was checked, so the certificate cannot be written up later and given an earlier date.

There are multiple types of records that sit in this stage. Each is stamped on Cardano as it is created, not when somebody comes looking for it.

1 CCTV and bodycam footage

WHAT GETS STAMPED ON CARDANO The footage as the recorder writes it, in short segments, each stamped with the camera identity and the time range it covers. Nothing is uploaded anywhere. The recorder keeps doing exactly what it does today.

The export becomes part of the system too. When a court asks for footage, PFMS hands over the original stamped segments exactly as the recorder wrote them, rather than building a new file.

WHAT IT PROVES A camera that was working leaves stamps. A camera that stops recording leaves a visible gap, flagged when it happens rather than discovered in court.



2 Distress call records

WHAT GETS STAMPED ON CARDANO The call recording and the incident entry, at the moment the call is logged. Then the dispatch entry, as it is made: which unit was sent and when it reached.

WHAT IT PROVES Whatever the entry said when it was made is what the stamp holds.

So if the time in the record today is the same time that was typed that night, it matches the stamp. If it was changed later, it does not. The recording works the same way. The audio saved on the night carries a stamp from the night, and any version that has been cut or edited since will not match it.

The question of what the control room recorded, and when, stops being an argument and becomes verifiable data.

3 ANPR (Automatic Number Plate Recognition)

WHAT GETS STAMPED ON CARDANO It captures the vehicle number plate details, as they are written into the ANPR database at the moment they are captured.

WHAT IT PROVES If a record gets added/deleted/modified in the ANPR database at a later stage then it can be checked against the stamped data on Cardano to rule out any tampering.

4 Patrol logs and the station diary

WHAT GETS STAMPED ON CARDANO Every entry the duty officer makes, at the moment it is made. Who came in, who was arrested, which van went where, and the time against each one.

WHAT IT PROVES Once an entry is stamped, it is settled. If it is edited or removed later, it no longer matches its stamp. If an entry is added afterwards, it has no stamp from that day behind it.

So what a court reads from the station record is what the station wrote on the day, and not a version of it.

5 Arms and ammunition records

WHAT GETS STAMPED ON CARDANO Every issue of a weapon or an ammunition and every return at the moment it is entered. The weapon, the officer it went to, the count of rounds out and the count back in.

WHAT IT PROVES The entry is stamped the moment it is made, so the count recorded that day is the count that stands. If it is changed afterwards, it no longer matches its stamp.

This protects the officer as much as the register. A record written correctly at the time can now be shown to have been written at the time.

6 Instrument calibration records

WHAT GETS STAMPED ON CARDANO The certificate on the day it is issued, with the instrument identity and the validity period.

WHAT IT PROVES The certificate now has a date that does not come from the certificate. It comes from the stamp, made on the day the instrument was actually checked, and nobody can move it afterwards.

So a certificate written on the day of calibration has a stamp from that day. A certificate written months later and given an earlier date has no stamp from that earlier date, because on that date it did not exist.

The two stop looking alike. When a reading is challenged, the court can see whether the instrument was checked before the reading was taken or after the question was asked.

STAGE TWO

2.4 Crime Investigation (FMS) (Proven on Cardano Mainnet)



1 The crime happens and the field forensic team arrives

The scene is taped off. The team photographs it and marks every item where it lies, before anything is touched.

2 Samples are collected

Each item is bagged and sealed on the spot. A random alias is generated for every sample as it is packed, so nothing on the packet points back to the case.

3 The case is opened and the secure QR is generated

At the station the case is registered and each box gets its own secure QR. Only the FMS app can read it. To anyone else it is just a code on a box.

4 Transported to the regional forensic laboratory

The sealed boxes travel by van to the laboratory, and every handover on the way is stamped. The lab receives boxes it cannot identify and tests them by alias alone.

From the moment a sample is bagged to the moment the laboratory reports on it, the evidence box carries only its alias. Nobody along the way can tell which case it belongs to, so there is nothing to target, and no way to swap or tamper with it unnoticed.

This stage is already proven on Cardano mainnet.

FMS hides the Case ID behind a secure QR that only the FMS app can read, generates a random alias for each piece of evidence so nothing on the box says which case it belongs to, and stamps every step from collection to laboratory on Cardano.

STAGE TWO · CRIME INVESTIGATION (FMS) · PROVEN ON CARDANO MAINNET

**It is successfully running currently with over
156,000 transactions on Cardano mainnet.**

FMS and PFMS Stage 2 do not measure the same thing. FMS, proven on Cardano mainnet in our previous deployment, secures one workflow: evidence moving from the crime scene to the forensic laboratory. PFMS Stage 2 in Telangana is wider in both coverage and scope.

Telangana, however, does not operate its forensic system in the same structure for which the existing FMS was built. Its laboratory network has a different organisational structure, includes district level mobile laboratories and custody transfers through forensic vans, and has its own instance of CCTNS.

PFMS therefore does not rebuild FMS. It takes the proven FMS engine and adapts it to Telangana's forensic and investigative architecture.

This approach allows PFMS to reuse what has already been proven on Cardano while building only the modules required to make that infrastructure work accordingly.

STAGE THREE

2.5 Evidence Storage Facility (Malkhana)



This is where evidence sits the longest, so it is where the record has to hold up the longest. Everything that happens to an item in this room is stamped on Cardano as it happens.

The secure QR

Every item that comes into the Malkhana is given its own QR code by PFMS, printed and pasted onto the packet. That code stays with the item for as long as it is in the room. The code identifies the record, not the object, so it is issued against a tamper evident seal whose identifier, intake photograph and condition are recorded at the same moment, and every handover is signed by both sides.

The code says nothing on its own. Read it with an ordinary phone and it gives nothing away. Read it inside the PFMS app, with an authorised login, and it opens the item's full record: what it is, which rack it sits on, when it came in, every time it has left the room and come back, and who signed for it at each point.

Every one of those events is fingerprinted and signed as it happens. So the record the QR opens is not a claim about the item's history. It is a history built entry by entry, each one signed as it was made.

The QR is also how the room runs day to day. The clerk scans it on intake, scans it on issue, scans it on return, and scans it during stock verification. Each scan writes the entry and stamps it in the same movement.



WHAT HAPPENS	WHAT GETS STAMPED ON CARDANO	WHAT IT PROVES
Intake and rack position	The QR is generated and pasted at this point. The item, its rack position and the intake entry are stamped together at the moment it goes on the shelf.	The item and the place it was put are tied together from the start, and that tie cannot be changed later. So a packet produced years afterwards can be matched back to the moment it went onto that rack. If the item and the entry no longer belong together, the stamp says so.
Every issue and return	Every movement out and back, recorded by scanning the QR, so the entry and the stamp are made in the same action as the handover. Who took it, when, and when it came back.	Each movement is signed as it is made, so the history of an exhibit builds up one stamped entry at a time. A record that runs across years becomes something a court can check rather than something it has to trust. And because the stamps run in sequence, a movement that was never entered leaves a gap between two of them.
Entry and exit registry	Every entry to the room, as it is made.	This record says the same thing on the day it is asked for as it said on the day it was written. It cannot be adjusted after the fact, which matters because the moment anyone asks who had access is always after the fact.
Stock verification	Each check, item by item as the QR codes are scanned, with what was found.	Every check becomes a fixed point in time. A check that came out clean can be proven to have come out clean on that date. And if something is later found missing, it can be placed between the last check that matched and the first that did not, so the loss has a window instead of no date at all.
Disposal and destruction	The destruction itself, signed as it happens, with the item's full history attached.	This is the only step in the chain with nothing left to inspect afterwards, because the item is gone. Stamping it as it happens leaves a permanent account of what was destroyed, when, and everything that had happened to it before. The item is gone. The record of it is not.

STAGE FOUR

2.6 Prosecution





Chargesheet

WHAT GETS STAMPED Every version as it is filed, including every supplementary chargesheet and every amendment.

WHAT IT PROVES Chargesheets are supposed to change. New evidence comes in, courts alter charges, High Courts strike parts out. None of that stops.

What changes is that version one still exists as a stamp. When the defence says a line is not what the March copy said, the March copy can be checked against its own stamp from March. A proper amendment shows as a new version in sequence. A page replaced quietly shows as a version that matches nothing.

Witness statements

WHAT GETS STAMPED The statement when it is recorded, with the date it was taken and the officer who took it.

WHAT IT PROVES The statement is stamped the moment the officer records it, along with the officer's identifier and the audio file of the statement. This ensures that the version in the file is the version that existed at that moment. If a line is changed later or a page is swapped, it no longer matches its stamp.

That takes one whole argument off the table. Nobody has to wonder anymore whether the statement was written after the fact or edited since.

Arrest and remand records

WHAT GETS STAMPED Times of arrest, production before a magistrate, and every extension of custody, as they are entered. The stamps carry through into the document filed in court.

WHAT IT PROVES The office being questioned still writes the record. It just can no longer change them later without the change showing.

Exhibit list and annexures

WHAT GETS STAMPED The list itself when it is filed. And the list is generated from the stamped Malkhana records rather than extracted from a central database.

WHAT IT PROVES Because the list is built from the stamped records, it cannot quietly disagree with them. Every item that was seized already has a stamp of its own, so an item left off the list has a stamp with nothing pointing to it, and an item on the list that was never seized has no stamp behind it.

The gap shows up on its own. Nobody has to go looking for it, and nobody has to notice.



STAGE FIVE

2.7 Court of Law



The judge no longer has to take the department's word on whether a record has been altered.

A record is produced, the verification layer checks it against its stamp, and it either matches or it does not. The verification layer answers that in moments, rather than across multiple hearings relying on third parties.

Where two records disagree, the stamps show which one changed and when. A question that used to run across years of adjournments becomes a single request to the verification layer.

2.8 What changes, in one sentence

WHAT CHANGES, IN ONE SENTENCE

Today, the truth and a lie can look exactly the same, and a person's life can depend on which one the court believes.

After PFMS, a record can prove it has not been changed since the day it was made.



3. Technical

PFMS is not a new system for the police to work inside. It is a massive state scale layer that sits on top of what the police already run.

3.1 The problem, and how PFMS answers it

All five stages run into the same problem. A record exists. It might be footage, a register entry, a calibration certificate or a filed document. Two years later a copy of it is produced in court, and there is no way to show that this copy is the one that was made at the time. PFMS handles that the same way at every stage.

We solve it by fingerprinting the record where it is made, on the recorder, at the terminal, or in the app in an officer's hand using a well designed sophisticated architecture. The fingerprint of the record is signed along with the device DID that made the record and the DID credential of the officer on duty, so all three arrive together as one signature instead of three separate claims and it is made in a highly resilient manner so even a station with no network can still sign and queue its records, and the fingerprints reach Cardano as soon as the link comes back.



Evidence Stack



3.2 TECHNICAL ARCHITECTURE · CONTINUED

Journey of the records

A record can start at any of the five stages on the left. From there it always travels the same way, through engines 01 to 05, onto Cardano, and out again at engine 06 when someone needs it proved. Each column reads downward: what arrives, what the engine does, and what it hands on.



4. Ecosystem Fit

4.1 Why Cardano

Every chain claims to be a good home for real world infrastructure. Very few have spent a decade building the specific things a system like this needs, and then proving them in production.

Cardano has produced blocks without interruption since launch, which for a system stamping evidence across every police station in the state is the difference between a record existing and a gap a defence lawyer will find.

The way transactions behave matters too. On Cardano, the outcome of a transaction is known before it is submitted. A stamp either goes through or it never left. There is no half state to reconcile, no silent failure discovered weeks later. Across thousands of capture points that reliability compounds into the thing that matters most, which is that nothing goes missing without anyone noticing.

Cardano gives PFMS something a departmental database alone cannot, a durable reference beyond the department's sole control. By stamping evidence fingerprints and identity registry commitments to Cardano, PFMS creates a reference that can be checked years later, even after officers, permissions and internal systems have changed. Cardano's decentralised network makes that possible, giving the verification layer a shared foundation that no single institution controls.

Then there is the question nobody asks until it matters: who could interfere with the record.

The whole point of stamping evidence outside the department is that nobody in the chain of evidence can reach it. That guarantee is only as strong as the chain's own decentralisation. If a handful of parties controlled block production, then in principle a handful of parties could be pressured, and the guarantee would be a matter of trust again rather than structure.

Cardano's Nakamoto Coefficient currently stands at 15, reflecting a highly decentralized network.

That decentralization is critical for PFMS. The proof of an evidence record does not sit with the police department, PFMS, or any single infrastructure provider. It is committed to a public network whose block production is distributed across independent stake pools.

For most applications, decentralization is a security property. For PFMS, it is what makes external verification credible.

Governance is the second half of the same argument.

The stamp made on the night a call came in has to still be provable long after the officers, the department heads and the government that commissioned this system have moved on.

Cardano is governed on chain under a constitution the community ratified. There is no company that can switch it off, no board that can lose interest, and no licence that can lapse. Protocol changes, treasury decisions and parameter updates all go through a public process with published rationale.

For infrastructure a state depends on for many years, that is a stronger guarantee than a service agreement with a supplier, because a supplier can be acquired, can fail, or can simply decide the contract is no longer worth renewing.

And it can be deployed by a public body without an argument about energy.

Cardano's proof of stake consensus means 1.53 million transactions a year from a state government carries an energy cost comparable to ordinary server infrastructure. A public institution deploying blockchain at this scale on a proof of work network would struggle to get past its own environmental procurement rules, and rightly so. On Cardano the question does not arise.



4.2 Cardano is already running chain of custody

None of this is theory. We have already built it, deployed it, and watched it work.

FMS covers one of the five stages: the journey from a crime scene to a forensic laboratory. It is proven on Cardano mainnet, has stamped more than 156,000 transactions there, currently runs at roughly 11,000 mainnet transactions a month, and ranks among the top ten applications on the [Cardano transaction leaderboard](#).

156,000+

transactions stamped on Cardano mainnet

1+ year

running live, every day, without exception

Behind every one of those 156,000 transactions is a real case, with a real person waiting to find out what happens to the rest of their life.

FMS has been running for over a year. It fits inside an existing procedure. It holds up in real conditions. And the chain has done exactly what was asked of it, every day, without exception.

So the question is not whether this works on Cardano. **That has already been established by FMS, which is proven on the Cardano mainnet.**

Both deployments are proven on Cardano mainnet under the addresses below. Every transaction, every count and every claim on this page can be checked on a Cardano explorer without asking us for anything. PFMS follows the same practice: the policy identifiers and contract addresses are published at M3, so the M3 and M4 evidence is checkable in exactly the same way.

FMS Forensic Management System, crime scene to laboratory
[addr1wynrwz69ne02lehp08y55wdmrsncv477tsv8t7uut506pwhk7wqr](#)

IndianChain Settlement infrastructure, Project Catalyst F14
[addr1w99se2k9d0vmdrz78qr2keekylgkk45dz3m8g0x2t1fl88chm4czv](#)

Chain of custody is running. The next step is the chain of evidence.



4.3 Impact

PFMS puts transactions and revenue onto Cardano, with every record sealed to the identity that produced it.

4.3.1 DID and Credential Registry

We are building the identity layer to structure the state's existing systems rather than replace them. We follow the schemas in accordance with existing systems such as CCTNS, which holds case and personnel records; NAFIS, which handles biometric identification; and PIS, which holds personnel information. Each has its own structure, custodian, and rules governing what may be held and who may access it.

The identity layer is built in accordance with CCTNS, NAFIS, and PIS, following their regulated structures so that an identifier in PFMS maps onto the record the department already maintains rather than competing with it.

The identity layer itself is held off chain. Personal data, personnel records, and biometric information are governed by these systems and remain within them.

Identity is bound in at the record level, before batching. The fingerprint of every record is signed together with the identifier of the device that produced it and the credential of the officer who created it, so the identity is part of the hash itself. Those signed fingerprints are then batched, and the Merkle root of the batch is what each transaction detailed in Section 4.3.2 commits to Cardano, together with the identifier of the source and a digest of the registry state in force at that moment. Identity is therefore not a separate stream of transactions sitting alongside the evidence. It is inside every fingerprint, and one batch carries the identities of every officer and device whose records it holds. So the question years later is not whether an officer is authorised now, but whether that credential was valid at the moment the record was stamped, and the fingerprint, the batch root and the registry digest together settle it through the verification layer.

≈1.93M

DIDs for facilities, devices, and staff

≈3.2M

evidence DIDs from cases and every item attached to them

≈5.1M

DIDs in the first deployment's registry (1.93M + 3.2M)



Not a single record can be stamped until the device and the officer behind it are registered. The identity layer therefore has to be complete for a station before that station produces anything. This covers every station, every evidence storage facility, every armoury, every registered device, and every officer who creates a record anywhere in the chain of evidence.

Types of DIDs in the Registry: First Deployment (Telangana)

The figures below are for Telangana, the first deployment. Each new jurisdiction adds its own facilities, devices, people and evidence to the registry.

CATEGORY	IDENTITIES
Facilities (Police Stations, Outposts, Evidence Storage Facilities, Armouries, Control Rooms, Forensic Laboratories, Mobile Forensic Vans, Prisons, Checkposts, Traffic Posts, Prosecution Offices, District Headquarters)	approx. 3,500
Devices (Police Station Cameras, Community CCTV, City Surveillance Cameras, ANPR Units, DVRs and NVRs, Bodycams, Dashcams, Breathalysers, TSCOP Handhelds, Patrol Vehicle GPS, Wireless Sets, Control Room Consoles, Station Terminals, Malkhana Scanners, Forensic Instruments)	approx. 1,810,000
People (Police Personnel, Home Guards, Control Room Operators, Traffic Personnel, Malkhana Clerks, Forensic Laboratory Staff, Prosecution Staff)	approx. 113,000
Evidences (New cases and every evidence item attached to them: physical exhibits, crime scene photographs, CCTV clips, seized devices, digital records, forensic samples, laboratory reports, chargesheets and annexures, witness statements, court orders)	approx. 3,200,000
TOTAL	approx. 5.1 million



4.3.2 Transactions on Cardano Mainnet

The projected transaction volume is driven by the continuous flow of operational data generated across the entire policing and justice ecosystem. Station activity, control room operations, traffic enforcement, evidence creation and custody transfers, forensic processes, prosecution records, and court side verification will all generate data that must be securely time stamped and verifiable on chain.

The transaction volume is therefore distributed across multiple high frequency workflows that operate every day across the system. Each record, evidence event, movement, verification, and institutional interaction is committed onchain in batches which contributes directly to on chain usage on Cardano mainnet.

The batching is specifically designed to preserve evidence integrity, based on requirements set by the state government about how quickly the evidence should be secured on Cardano. Shorter windows mean the evidence is secured sooner, while longer windows would leave the evidence dependent on off-chain custody for longer. Batching intervals are randomised for security reasons rather than fixed, so no source commits on a predictable schedule. The transaction count is a result of this process.

Based on the expected volume of data that will be stamped across all of the above workflows, the system is projected to generate approximately **1,530,000 Cardano Mainnet Transactions in its first year**, a figure expected to grow with adoption.

We built this projection from the state's own record volumes for the first year, one stage and one source at a time. It counts only the sources and record kinds that are part of the system at launch. This makes 1,530,000 a conservative floor for the first year, not the figure the system will reach when it is fully in use.

The number grows from there because of how the state adopts new systems. Telangana brings new police technology into use commissionerate by commissionerate and district by district, and PFMS will follow the same path. Each new commissionerate or district that comes on board adds its stations, cameras, devices and officers to the registry, and each of them starts sending its own commits. The number also grows when new kinds of record are added after launch, and every year as new cases bring new exhibits, handovers and filings. Each further jurisdiction that adopts PFMS adds its own volume on top.

**WHERE THE TRANSACTIONS COME FROM: FIRST DEPLOYMENT**

WHAT IS STAMPED	CARDANO MAINNET TRANSACTIONS, YEAR ONE
CCTV and bodycam recordings, control room call logs and dispatch entries, ANPR captures, patrol logs and station diary, armoury issue and return, breathalyser and instrument calibration, etc.	630,000
Crime scene collection, evidence sealing and labelling, FSL transfers, forensic van custody, lab test reports, evidence entries created, etc.	420,000
Exhibit intake and QR tagging, rack allocation, issue to court or lab, return, entry and exit registry, stock verification, disposal and destruction, etc.	315,000
Chargesheet and supplementary chargesheet versions, witness statements, arrest and custody records, exhibit lists and annexures, etc.	105,000
Exhibit receipts, remand and custody extension orders, witness depositions recorded in trial, charge alteration orders, disposal orders, etc.	60,000
TOTAL	at least 1,530,000



4.4 What it means for Cardano

The numbers above are what PFMS produces. This is what they mean for the network.

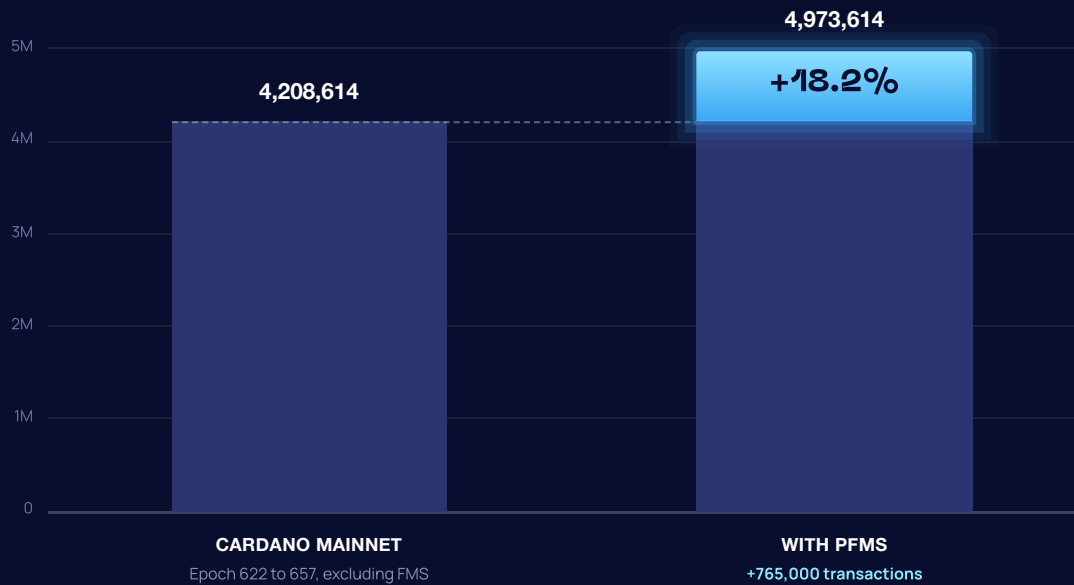
Cardano currently processes around 118,643 transactions per epoch. Over the six months from Epoch 622 to Epoch 657, the network handled 4,271,138 transactions in total. FMS is already part of that figure, so the baseline used below is 4,208,614, the network total with FMS taken out, and nothing is counted twice.

The table below sets PFMS against that baseline, alongside our existing deployments.

	CARDANO MAINNET (EXCL. FMS)	FMS	INDIANCHAIN	PFMS (PROJECTED, FIRST DEPLOYMENT)	TRIVOLVE TOTAL
One epoch	116,906	~1,737	2,311	~20,959	~25,007
One month (~6 epochs)	701,436	~10,421	~20,000	~127,500	~157,921
Three months (~18 epochs)	2,104,307	~31,262	~60,000	~382,500	~473,762
Six months (~36 epochs)	4,208,614	62,524	~120,000	~765,000	~947,524

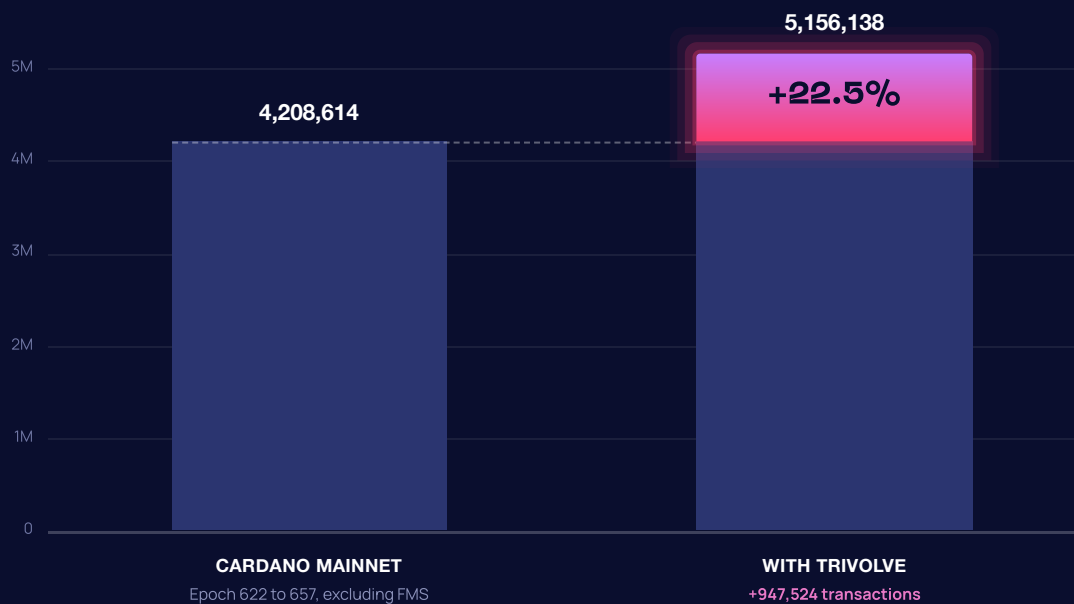


Cardano mainnet transactions with PFMS



That is worth sitting with for a moment. Not eighteen percent from a trading venue, or a token launch, or activity that arrives with a market cycle and leaves with it. Eighteen percent from a single state government doing the ordinary work of criminal justice and it is the beginning rather than the ceiling.

Cardano mainnet transactions with all Trivolve deployments





4.5 Revenue Potential Beyond Transactions

Cardano not only gets transaction fees, but also has high potential for further revenue from the verification layer.

How the revenue would work

PFMS will offer a paid verification service to authorised parties, such as registered defence lawyers and the prosecution. Once live, parties involved in a case will be able to verify the chain of evidence by paying a verification fee. All revenue generated from these verifications is committed as follows: 70% is returned to the Cardano Treasury, 20% funds core Cardano library maintenance, and 10% goes to Trivolve Tech.

Each verification request carries a charge. Based on our model, the absolute minimum price per request starts at **\$1.89**, applicable to the smallest and simplest verification requests. Pricing scales with the size, complexity, and volume of the dataset being verified, meaning a single verification request can reach several hundred dollars when large datasets or extensive case histories are involved.

This paid verification is an optional, fast tracked service. It runs alongside the regular verification process, not in place of it. Anyone who does not use it can still have records checked through the existing process. Those who choose it simply get a faster, fully documented answer, in the same way a priority service sits alongside a standard one.

70% of this revenue is returned to the Cardano Treasury, 20% funds core Cardano library maintenance and 10% goes to Trivolve Tech.

From \$1.89 minimum charge per verification request	Hundreds of dollars per verification request, scaling with request size and the dataset being checked	70% returned to the Cardano Treasury	20% funds core Cardano library maintenance. The remaining 10% goes to Trivolve Tech
---	---	--	---

To keep this fully transparent, at the end of every month, every paid request is stamped through the verification layer on Cardano mainnet with its fee and price tier, without any case details or requester identity.



4.6 Cardano 2030 KPI Alignment

The PFMS directly supports the Cardano 2030 KPIs and Strategic Pillars by driving substantial mainnet transaction volume, expanding decentralized identity usage, and generating recurring protocol and verification revenue.

KPI / METRIC	2030 TARGET	PFMS CONTRIBUTION	ALIGNMENT & DIRECT IMPACT
Monthly Transactions	≥ 27 Million / month	~127,500 transactions/month in Telangana alone during Year 1 (≥ 1.53 Million annually)	Adds 18.2% to today's Cardano mainnet monthly transaction baseline. Grows further as more districts, record types, and additional Indian states are onboarded.
Annual Protocol Revenue	> 16 Million ADA	100% of transaction fees paid by the state government, plus 70% of data verification revenue returned to the Cardano Treasury	Transaction commit fees are paid continuously by the state government regardless of market cycles. Data verifications generate revenues for Cardano Treasury.

PILLAR	HOW PFMS ALIGNS	CONTRIBUTION STRENGTH
Pillar 2: Adoption & Utility	Invisible Technology: Runs quietly in the background without altering existing officer workflows. Decentralized Identity: Registers ~5.1 Million DIDs across facilities, hardware, personnel, and evidence items, keeping sensitive personal data off-chain. Provenance: Secures end to end evidence chain provenance from pre-crime capture to court verdict. Open-source Incentives: 20% of revenue from verification layer is directed to maintaining the open-source Cardano libraries, supporting a sustainable builder ecosystem.	Primary
Pillar 4: Community & Ecosystem Growth	Demonstrates Enterprise Value: Scales chain of evidence tracking across an entire state government ecosystem. Reusable Model: Open source core engine allows easy expansion to rest of India's 35 states and union territories without additional build costs to the Treasury.	Strong
Pillar 5: Sustainability & Resilience	Financial Stewardship: The Cardano Treasury funds a one-time build, while ongoing transaction costs, infrastructure, and maintenance are funded entirely by the state governments as PFMS is rolled out to more states, starting with Telangana.	Strong



5. Team and Track Record

5.1 Trivolve Tech (Trivolve Tech Pvt Ltd)

TRIVOLVE
Tech

Trivolve Tech

Blockchain and AI development studio · enterprise and government deployments

trivolvetechnology.com

Trivolve Tech is a blockchain and AI development studio focused on building and deploying enterprise grade solutions across government, healthcare, fintech, decentralized finance, and real world assets.

Over the past three years, our team has delivered 30+ projects for enterprises, governments, venture capital firms, and Fortune 500 companies. Our experience is not limited to prototypes or proof of concepts. We specialize in taking complex operational systems and deploying them at production scale, where reliability, auditability, security, and long term maintainability are critical.

30+projects delivered in three
years**42**

dedicated professionals

156,000+transactions on Cardano
mainnet**2**

state government systems live

Our track record on Cardano demonstrates this ability.

01

Trivolve Tech built a Forensic Management System that became **the first ever enterprise grade project on Cardano to surpass both the 100,000 and 150,000 transaction milestones on Cardano Mainnet**. This deployment demonstrates our ability to operate blockchain infrastructure at production scale.

02

We subsequently delivered another large scale government deployment through **IndianChain, bringing an entire Indian state government's agriculture sector onto Cardano**. Launched on Cardano Mainnet in September 2026, it has already processed over 15,000 transactions and ranks among the top ten applications on the [Cardano transaction leaderboard](#). This gives us direct experience in navigating government requirements, institutional stakeholders, operational workflows, and blockchain infrastructure within a live public sector environment.

03

Our experience also extends beyond software deployments. Trivolve Tech was **the first blockchain company involved in the tokenization of granite on Cardano**, giving our team practical experience in bringing physical real world assets and industrial processes into blockchain based systems.

Today, Trivolve Tech has a dedicated team of 42 professionals with deep expertise spanning:

Blockchain infrastructure and enterprise deployments

Government systems and policy requirements

Artificial intelligence and data systems

DeFi and Web3 infrastructure

Enterprise software

Fintech and financial infrastructure

Healthcare technology

Real world asset tokenization

Systems integration and automation

This combination of technical depth and implementation experience allows us to work across the full lifecycle of a project, from architecture and development to integration, deployment, and production operations.



5.2 Quixy (Vivid Minds Pvt Ltd)



Quixy

No code / low code application development and business process automation platform

quixy.com

Trivolve Tech is complemented by Quixy as a subcontractor, a leading no code and low code application development and business process automation platform serving governments and enterprises worldwide.

Quixy's experience provides the enterprise application and workflow layer required to transform complex organizational processes into scalable digital systems. The platform has enabled the development of 27,000+ applications, serving 200,000+ users across 15+ industries.

27,000+

applications built on the platform

200,000+

users served worldwide

15+

industries covered

This brings a critical capability to the project: the ability to translate complex institutional processes into practical, scalable applications that can be adopted by large organizations and government stakeholders.

5.3 A Team Built for This Scale

The strength of this partnership comes from the combination of two complementary capabilities.

Trivolve Tech brings deep blockchain expertise, Cardano Mainnet deployment experience, government technology experience, AI capabilities, and real world asset infrastructure.

We understand the technical requirements of Cardano. We understand the operational realities of government systems. We understand enterprise scale application development. And we have already demonstrated our ability to take these technologies from concept to production.



5.4 Who owns PFMS

The entire PFMS codebase will be released as open source as a public good. Trivolve Tech is the developer and maintainer of PFMS.

Only two things are kept private, and both are specific to a deployment rather than part of the product. The first is each state's connector configuration modules, which describe the police systems that state actually runs. The second is the signing keys and credentials held by whoever operates the system. Everything that makes PFMS work is public.

OPEN SOURCE ON CARDANO

All the six engines, the stage smart contracts, the DID registry, the verification layer, the batch commit format, the record definitions and every test vector.

KEPT PRIVATE

Each state's connector configuration modules, which describe that state's police systems, and all signing keys and credentials.

More than one state, within the same budget

India has 36 states and union territories. The engines, the smart contracts, the DID registry and the verification layer carry over unchanged from one state to the next. Only the state specific minor integration modules will be changed. Within the scope of this proposal we will put in the effort to deploy the same solution to multiple states of India, and we will not come back to the Treasury for a top up in order to do it.

How each government uses it, and what it pays

The government is the user of PFMS. It pays for all the infrastructure it runs and for the Cardano transaction fees of every commit it produces.

WHAT	WHO PAYS	WHAT IT COVERS
Building PFMS	Cardano Treasury	A one time build, funded by this proposal. Nothing further is asked of the Treasury.
Cardano transaction fees	The state	Paid to Trivolve Tech in fiat. Trivolve Tech takes no margin. As the maintainer of the product, Trivolve Tech converts it and pays the fees in ADA for every commit the state produces.
Infrastructure	The state	Servers and storage, network and connectivity, the capture devices at each source, the Cardano nodes and the signer service, backups and disaster recovery from the build period onward.
Maintenance	The state	Paid to Trivolve Tech and its subcontractors for bug fixes, security patches, upgrades, monitoring and helpdesk, under a separate agreement with the state.
Verification revenue	Requesting Parties	70% is returned to the Cardano Treasury, 20% funds core Cardano library maintenance and 10% goes to Trivolve Tech.



5.4 WHO OWNS PFMS · CONTINUED

Why the Treasury funds the build

The Treasury is not paying for software that is specific to, or owned by, one Indian state. It is paying for the part of PFMS that belongs to the ecosystem: an open source evidence layer that runs on Cardano. It is a public good, with use cases that reach beyond India and beyond police work, and every future jurisdiction adopts it without another build.

Treasury funding is what puts the chain of evidence on Cardano mainnet, and keeps the core open for every project that follows. Trivolve Tech and its subcontractors receive no fees or compensation from the state government for building PFMS. The Treasury is the sole funder of the build.

The state carries the physical deployment, pays every transaction fee and runs the system on its own infrastructure. Cardano earns the fees, receives 70% of verification revenue, and gets a reusable system at no further build cost.

A government ecosystem on Cardano

Every state that adopts PFMS brings its record volume onto Cardano mainnet, and brings its institutions into contact with the chain: police, forensic laboratories, evidence storage, prosecution and the courts. What is being built is not a single deployment. It is a government ecosystem around Cardano, with its core open to everyone.



6. Funding Ask

6.1 The ask, in plain terms

9,600,000 ADA

over 15 months.

At a planning rate of USD 0.23 per ADA, that is USD 2.208 million. The amounts in this proposal are fixed in ADA. The dollar figures are planning references only. Project expenditure is hard capped at USD 0.30 per ADA, which is USD 2,880,000 on the 9,600,000 ADA ask, and any value above that cap is returned to the Cardano Treasury (Section 8.4).

That covers everything described in this proposal. Building all five stages of PFMS. Integrating with the systems the state already runs and launching on Cardano mainnet.

Once PFMS is live on Cardano mainnet, the first deployment alone will produce at least 1.53 million Cardano mainnet transactions in its first year, a figure expected to grow with adoption.

6.2 Disbursement schedule

Five tranches. One on administrator contract signing, four on verified milestone completion.

1.8M Kickoff	2M Month 3	2M Month 8	2M Month 12	1.8M Month 15
contract signing				month 15
TRANCHE	RELEASED			ADA
Milestone 0 (Kickoff)	On administrator contract signing			1,800,000
Milestone 1: Foundations	Month 3			2,000,000
Milestone 2: Proven on Cardano Preprod	Month 8			2,000,000
Milestone 3: Tested and on Mainnet	Month 12			2,000,000
Milestone 4: Sustained Usage	Month 15			1,800,000

Tranches for Milestones 1 to 4 are released only after the deliverables for the corresponding milestone have been verified by the independent assurer and the administrator and reported to the community.



6.3 Budget Allocation

The ask is 9,600,000 ADA over fifteen months. The budget directly funds the design, development and deployment of the six engines and five stage modules, the stage smart contracts and DID registry, the read-only connectors into the source systems, and the edge agent that captures records at the point they are created. It also covers end-to-end testing, mainnet load proving, the final handover package, rigorous penetration testing, the independent assurer and audit, the Cardano Foundation's administration, and overall project delivery and management. Every budget line maps to the work packages set out in Section 6.4, while the milestones in Section 6.5 define when each component becomes eligible for payment.

LINE	ADA	USD AT 0.23	SHARE
Core blockchain and identity infrastructure	2,688,000	\$618,240	28%
Stage module engineering	2,112,000	\$485,760	22%
Integration test engineering, load proving and handover	1,536,000	\$353,280	16%
Systems integration	1,152,000	\$264,960	12%
Edge capture and resilience engineering	960,000	\$220,800	10%
Security testing	472,000	\$108,560	4.92%
Project management & audit	480,000	\$110,400	5%
Administration	200,000	\$46,000	2.08%
TOTAL	9,600,000	\$2,208,000	100%

All amounts are fixed in ADA. The USD column is a planning reference at 0.23. Expenditure is hard capped at USD 0.30 per ADA, which is USD 2,880,000 (Section 8.4).



Each work package below draws on one or two of the budget lines in section 6.3. The lines are drawn so that no two of them pay for the same thing, and the milestone tables in section 6.5 show when each part of the work is accepted and paid.

6.4 Work Packages

The 15 month programme is organised into eight work packages. Six of them build the six engines described in Section 3.2, one engine each, in the order a record travels through them. The seventh puts those engines to work in the five stages of a case and proves them end to end on mainnet. The eighth carries security, independent assurance and governance across the whole period.

#	WORK PACKAGE	ENGINE	PRINCIPAL ACCEPTANCE
WP1	Source Engine: Record Definitions, Field Schemas and Version Registry	01	M1
WP2	Capture Engine: Edge Agent, Store and Forward Queue and Read Only Connectors	02	M2
WP3	Identity Engine: DID Registry, Officer Credentials and Device Identities	03	M2
WP4	Stamping Engine: Fingerprints, Combined Signatures, Batching and Completeness Counts	04	M2
WP5	Commit Engine: Stage Smart Contracts, Mainnet Submission and Signer Service	05	M3
WP6	Verification Engine: Proof Bundles, Verification Layer and Evidence Trail Documents	06	M3
WP7	Five Stage Modules, End to End Testing, Mainnet Load Proving and Handover	Across all	M2 to M4
WP8	Penetration Testing, Open Source Release, Independent Assurance, Governance and Reporting	Across all	M4

Each package states its scope, its deliverables, the evidence by which delivery is judged, and what it depends on. The budget line each package draws on is set out in Section 6.3.



WP1: Source Engine, Record Definitions, Field Schemas and Version Registry

Scope. A record can only be stamped if the system knows what it is. This package writes down every kind of record that PFMS will handle. Numerous distinct record kinds run across the five stages of a case, among them camera footage, control room call and dispatch entries, station diary entries, ANPR captures, armoury issue and return, instrument calibration certificates, crime scene and forensic transfer records, Malkhana movements, prosecution filings, court orders, etc. For each kind the definition states where the record starts and ends, what its fields mean, and what its date and time refer to at that source.

Every definition is versioned. When a definition changes later, records stamped under the earlier version still check, because the version they were stamped under is written into the stamp itself.

Deliverables.

- A written definition for every record kind, checked against real samples of that record.
- A version registry, so that every definition carries a version number and every stamp names the version it used.
- Test vectors for every record kind: sample records and the fingerprint each one must produce, published.
- A guide to testing a record end to end and how to reproduce its fingerprint and check it against Cardano.

Evidence. Working artifacts: the published definitions, the version registry and the test vectors. Reproducible test: a sample record of each kind parses cleanly against its definition, with every field and its timestamp resolved, demonstrated at review.

Dependencies. Records from each source system, which the state has already provided. WP2 and WP4 build on these definitions and cannot be accepted before them.

WP2: Capture Engine, Edge Agent, Store and Forward Queue and Read Only Connectors

Scope. This package builds the software that sits where a record is born. The edge agent runs beside the recorder or the terminal and hashes the raw bytes of a record at the moment they are written, so the file is never converted or saved again, and nothing waits. That hash, with the record's identity, is what the stamping engine in WP4 seals and batches. A store and forward queue holds fingerprints in numbered order on the device and sends them up when the link returns, so a capture point with no network still signs and still queues. Cardano fixes the outer bound. The block that carries a fingerprint proves the record existed by that block, fixed by the network and beyond anyone's reach to move. Three times are kept for every record: the event time claimed by the source, the signing time taken from a synchronised network clock with the device's drift recorded against it, and the block time on Cardano. The first two are signed claims and the third bounds them. The permitted clock error is set per record kind, and a record that exceeds it is committed with its drift declared rather than silently accepted.

The connectors are the other half. They read from the systems the state already runs: CCTNS, DVR and NVR recording systems, control room and voice logging systems, ANPR databases, station diary systems, armoury systems, and the prosecution and court systems. Every connector is read only. It watches for the moment a record is committed in the source system and reads it. It never writes anything back.

WP2: CAPTURE ENGINE · CONTINUED

Deliverables.

- The edge agent, deployable on any capture point, hashing at write and holding a numbered local queue that survives a restart and an extended loss of network.
- Cardano block time as the outer bound for every fingerprint, with the claimed event time, the device signing time, and the permitted clock error all recorded alongside.
- Read only connectors for each source system listed above, built on one shared connector framework so a new source can be added without new core code.
- An induced failure test: the link is cut, records keep queuing, the link returns, and every record is committed in order with the gap visible and then closed.

Evidence. Working artifacts: tagged releases of the agent and the connectors. Reproducible test: the induced failure test shows that no record is lost and none is reordered, and a read only test in which the source system is checked before and after shows no change. On chain data: fingerprints from live capture points committed on preprod at M2 and on mainnet at M3.

Dependencies. WP1 for the record definitions. WP4 for the fingerprint and batch format. A test instance of each source system, arranged with the state.

WP3: Identity Engine, DID Registry, Officer Credentials and Device Identities

Scope. Nothing can be stamped until the device that made the record and the officer who was on duty are both known. This package builds the credential registry that answers those two questions. It is built on the systems the department already keeps, CCTNS, NAFIS and PIS, and it does not copy personal data out of them. It issues a DID and a signing key to every camera, recorder and terminal before that device can sign anything, and it carries each officer's role, station and the period for which the credential is valid.

The registry is held off chain. What reaches Cardano is a single value that stands for the whole registry at a point in time, carried inside every stamp. A court can later confirm that a device and an officer were valid on the day a record was made, without anyone reading the registry itself.

Deliverables.

- The credential registry, with its data model built to the CCTNS, NAFIS and PIS schemas.
- Device identity issuance, so that every capture device holds a DID and a signing key before it enters the signing path.
- Officer credentials carrying role, station, scope and validity period, each version with the interval it applies to, and a revocation path for when a credential ends.
- The registry state digest, computed on a fixed schedule, published as each version takes effect and carried in every batch commit, so a state cannot be constructed after the fact to authorise a signature.
- The DID issuance, rotation and revocation service for devices and officers, built to the CCTNS, NAFIS and PIS schemas.

Evidence. Working artifacts: the registry, its schema and the issuance and revocation service. A record signed against a registry version older than a revocation is accepted only at reduced assurance and reported as such. Reproducible test: a test credential is revoked, records signed against a later registry version fail verification, and records signed offline against an earlier version are reported at reduced assurance, demonstrated at review. On chain data: registry digests inside committed batches. No personal data, personnel record or biometric appears in any evidence.

Dependencies. Read access to CCTNS, NAFIS and PIS reference data, already received from the state.

WP4: Stamping Engine, Fingerprints, Combined Signatures, Batching and Completeness Counts

Scope. This package takes a record and the identities attached to it and turns them into something that can be written to Cardano and checked years later. It does five things. First, it lays every record of a given kind out in a fixed order before fingerprinting it, so the same record always produces the same fingerprint whichever system exported it. Second, it signs the record, the device and the officer together as a single unit, so nobody can keep the record and change who made it. Third, it combines all the fingerprints from one source over one window into one summarised string of hashes, the Merkle root. Fourth, it counts the records expected, captured and sealed in that window, so a silent camera is noticed. Fifth, it versions every layout, so a seal from year one still checks in year ten.

Deliverables.

- The canonicaliser, which produces the fixed form for each record kind defined in WP1.
- The signing path that seals record, device and officer into one signature.
- The batcher, which builds one summarised string of hashes per source per window.
- The reconciler, which reports expected against captured against sealed for every source and every window.
- The version rule, so that a change to any form does not invalidate what was already stamped.

Evidence. Reproducible test: a record run through the canonicaliser produces the same fingerprint every time, and altering one byte changes the fingerprint. A version bump test: a form is revised, and records stamped under the earlier version still verify. Working artifacts: tagged releases and the batch format specification. On chain data: batches committed with their hashes.

Dependencies. WP1 for the definitions. WP3 for the identities that are sealed in.

WP5: Commit Engine, Stage Smart Contracts, Mainnet Submission and Signer Service

Scope. This package writes the hashes to Cardano mainnet and builds the rules that live there. Records are committed in batches at every stage, grouped by source and by window. Each commit carries the summarised string of hashes, the window, the record count and the registry state at the time, and the state is partitioned so that sources commit concurrently. The block it lands in proves every record inside it existed by that block. The contracts check the transitions carried inside each batch against the state the previous batch left behind, so a move that is not allowed does not change the state. The batch still lands, and the attempt is recorded on chain as a rejected transition, carrying the same signed identity binding as any other record. Each stage has multiple smart contracts to enforce multiple sets of rules such as capture rules accept a capture only from a device holding a valid DID inside a closed window. Only fingerprints, summarised strings of hashes, digests and counts go on chain.

Deliverables.

- The batch commit format and the full set of stage smart contracts, covering every rule each stage needs, written and tested on preprod.
- The committed custody state and the validator that enforces the exhibit state machine inside each batch.
- The signer service and the submission infrastructure, with multi signature signing so that no single key can commit alone.
- A Cardano node operated for PFMS, with monitoring.
- The contract set frozen at M2 and ready for penetration testing, and deployed to mainnet only after every finding has been fixed and retested.

Evidence. On chain data: contract addresses, policy identifiers, transaction hashes and counts, on preprod through M2 and on mainnet from M3. Reports: the penetration test report and its remediation record. Reproducible test: a handover that breaks a rule, for example issuing an exhibit that was never returned, leaves the exhibit unmoved and appears on chain as a rejected attempt, demonstrated at review.

Dependencies. WP4 for the batch contents. WP3 for the registry digest. WP8 for the penetration testing that gates deployment to mainnet.



WP6: Verification Engine, Proof Bundles, Verification Layer and Evidence Trail Documents

Scope. Everything before this point exists so that a check can be made later. This package builds that check. It builds the verification layer, which takes a request for any stamped record, reads its proof against Cardano directly, and fails if a single byte has changed. It returns the evidence bundle: the record, the proof that it sat inside a stamped batch, and a reference to the transaction that carried it. And it builds the evidence trail document it returns alongside: what checked out, what did not, which registry version was in force, and whether the officer's credential was valid and unrevoked at the time.

Every check runs through the verification layer, which reads the proof against Cardano directly. Prosecution, defence and the judge each request the same record and receive the same bundle.

Deliverables.

- The evidence bundle format, assembled by the verification layer for any stamped record on request.
- The verification layer, which takes a request from prosecution, defence or the court and checks the record directly against Cardano.
- The evidence trail document, in plain language, returned by the verification layer.
- Written documentation on how to request a record and how to read the evidence trail document returned.

Evidence. Reproducible test: a record returns a bundle that verifies, and altering one byte of the record makes the verification fail, demonstrated at review. Working artifacts: the verification layer and its documentation. Reports: sample evidence trail documents returned for real stamped records, on preprod at M2 and on mainnet at M3.

Dependencies. WP5 for the commit format the proof points to. WP4 for the batch format. WP3 for the credential validity check.

WP7: Five Stage Modules, End to End Testing, Mainnet Load Proving and Handover

Scope. The six engines are shared by every stage. This package builds what each stage needs on top of them, and then rolls the whole system out. Stage 1 gets the six Pre-Crime record modules, for cameras, control rooms, ANPR, station registers, armouries and instruments. Stage 2 builds on our FMS work, which is already proven on Cardano mainnet, and extends it to this state's laboratory network, its forensic vans and the CCTNS instance in use. Stage 3 gets the Malkhana module, with QR intake, issue and return, stock verification and disposal. Stage 4 gets the chargesheet versioning, witness statement, arrest and remand, and exhibit list modules. Stage 5 gets the court verification report.

Testing goes stage by stage. Each module is run against real records from the source systems, the connectors are exercised end to end, and every failure mode is provoked on purpose: a dropped link, a stopped camera, an exhibit issued twice. Load is then proven on mainnet: 100,000 transactions produced by records captured from live sources through the deployed contracts.

Deliverables.

- The Stage 1 record modules, the Stage 2 investigation modules, the Stage 3 Malkhana module, the Stage 4 prosecution modules and the Stage 5 court module, each tested end to end and accepted.
- The integrated pipeline: one record travelling from any stage through all six engines and out to an evidence trail document.
- End to end test results for every stage and every record kind, with every failure mode provoked and recovered.
- Load proving on mainnet: 100,000 transactions from live sources, with the reconciler showing no gap.
- A technical guide for each stage on how to check a record and read the result.

Evidence. On chain data: transactions from live sources on mainnet, with counts per source and per window. Reports: test reports for each stage and the load proving report. Reproducible test: one record is followed from capture to its evidence trail document and confirmed by the verification layer at the far end, and one exhibit is followed through every custody handover from intake to disposal.



WP7: STAGE MODULES · CONTINUED

Dependencies. All six engine packages. WP8 for the penetration testing that must pass before anything reaches mainnet.

WP8: Penetration Testing, Open Source Release, Independent Assurance, Governance and Reporting

Scope. This package runs across the whole period. It procures the independent assurer as soon as the first tranche is released and publishes the procurement. It covers penetration testing at M2, covering the stage smart contracts and the signer service as well as the edge agent, the connectors and the registry services, and sees every finding fixed and retested before anything reaches mainnet. It publishes the PFMS core codebase under the Apache License 2.0 at M3, once penetration testing and mainnet deployment are complete, and completes the open source handover at M4 with the final tagged production release. It keeps the accounts, reports every milestone, and returns unspent funds.

Deliverables.

- Independent assurer procured through competitive procurement, with the shortlist, the selection basis and the confirmation of no conflict of interest published.
- Threat model and security architecture review, reported in summary.
- Penetration testing of the stage smart contracts, the signer service, the edge agent, the connectors and the registry services, with every finding fixed and retested before deployment to mainnet.
- Open source release at M3: the six engines, the stage smart contracts, the DID registry, the verification layer, the batch format and the test vectors published under the Apache License 2.0, while state specific connector configurations, signing keys and credentials are kept private.
- Final open source handover at M4: the final tagged production release, technical documentation, deployment guides, reproducible tests and all five stage modules in the public repository.
- Milestone reports at M1, M2, M3 and M4, and a final reconciliation with the return of unspent ADA.

Evidence. Reports: the procurement record, the penetration test report and its remediation record, assurer reviews and milestone reports. Public repository: the tagged releases, the licence and the reproducible build and test documentation. On chain data: treasury movements and milestone disbursements.

Dependencies. Runs across every package. Penetration testing and its fixes should complete before WP5 deploys to mainnet.

6.5 Milestones and Acceptance

Delivery is structured around a kickoff tranche and four delivery milestones across the 15 month funded period. Each milestone has named acceptance evidence. The first tranche (Milestone 0, Kickoff) is released on administrator contract signing.

MILESTONE	TIMING	COVERAGE	PAYMENT RELEASED
M0 Kickoff	On administrator contract signing	Kickoff tranche	1,800,000 ADA
M1 Foundations	Month 3	All record kinds defined and versioned with test vectors; contracts running on preprod; credential registry exercised on test data	2,000,000 ADA
M2 Proven on Cardano Preprod	Month 8	One record end to end through all six engines on preprod for Stages 1 to 3; contract set frozen and submitted for penetration testing	2,000,000 ADA
M3 Tested and on Mainnet	Month 12	Penetration testing passed; contracts on mainnet; all five stages tested end to end and accepted; verification layer live; 100,000 transactions from live sources on mainnet; codebase open sourced	2,000,000 ADA
M4 Sustained Usage	Month 15	At least 390,000 transactions from live sources across all five stages in 3 months; open source handover	1,800,000 ADA



The gate. The independent assurer is procured as soon as the first tranche is released, and the procurement is made public: the shortlist, the selection basis, the appointed assurer and its written confirmation that there is no conflict of interest are all published. The assurer reviews every milestone from M1 onward. No milestone tranche is released until the independent assurer and the Cardano Foundation, as administrator, have verified that milestone's deliverables and they have been reported to the community (Section 7).

M1: Foundations (Month 3)

M1 covers the groundwork that must be in place before anything is built on top of it. All record types listed in the table in Section 4.3.2 are documented across facilities, devices, people and evidences, versioned and published along with test vectors, so that from this point onward the same record always produces the same fingerprint, whichever system it came from. The stage smart contracts are written and running on preprod. The credential registry is in place, with its data model built to the CCTNS, NAFIS and PIS schemas, and is exercised on test data. The edge agent exists as a prototype and has passed its first induced failure test. No contract reaches mainnet during this period.

DELIVERABLE	WP	EVIDENCE TYPE
All record types in Section 4.3.2 defined, versioned and published with test vectors	WP1	Working artifacts + reproducible test
Edge agent prototype hashing at write, with the induced failure test passed in the lab	WP2	Reproducible test
Credential registry built to the CCTNS, NAFIS and PIS schemas and exercised on test data	WP3	Working artifacts
Canonicaliser and signing path producing the same fingerprints on every run	WP4	Reproducible test
Contracts for the capture, transit, custody and filing rules running on preprod	WP5	On chain data (preprod)
Independent assurer procured and the procurement published	WP8	Reports
M1 milestone report	WP8	Reports

The definitions and the registry are shown as working artifacts. The fingerprints and the induced failure are shown as tests that run and pass. The contracts are shown as data on preprod. The procurement is shown as a published record. The gate is that the foundations are correct. It is not a volume gate.

M2: Proven on Cardano Preprod (Month 8)

At M2 a single record shall travel the entire length of the system. A record captured from a working source system shall pass through all six engines and emerge as an evidence trail document, which the verification layer shall confirm against preprod. This shall be demonstrated for Stages 1 to 3, namely the Pre-Crime records, the investigation records and the Malkhana. The connectors shall read from test instances of the source systems. DIDs shall be issued to the test set of devices and officers. The contract set shall be frozen for penetration testing. Nothing shall reach mainnet in this period, and this is by design.

DELIVERABLE	WP	EVIDENCE TYPE
Edge agent and read only connectors running against test instances of each source system	WP2	Working artifacts + on chain data (preprod)
DIDs issued to the test set of devices and officers, with revocation tested	WP3	Reproducible test
Batches carrying summarised strings of hashes, counts and registry digests committed on preprod for every Stage 1 to 3 source	WP4, WP5	On chain data (preprod)
Contract set frozen and ready for rigorous penetration testing	WP5, WP8	Reports
Verification layer returning bundles and evidence trail documents from preprod records	WP6	Reproducible test
Stage 1, 2 and 3 modules delivered and tested end to end	WP7	Reproducible test + working artifacts
M2 milestone report	WP8	Reports



M2: PROVEN ON CARDANO PREPROD · CONTINUED

Every engine has run against a real record from a real source, and the result has been confirmed by the verification layer at the far end.

M3: Tested and on Mainnet (Month 12)

At M3 the system goes live on Cardano mainnet. Penetration testing is complete, every finding is fixed, and the fixes are retested before anything is deployed. All five stages are tested and accepted. DIDs are issued for all categories, and load is proven by producing 100,000 transactions from live sources through the deployed contracts. The policy identifier and the contract addresses are published at this milestone, so every transaction made from here on can be queried.

Following successful penetration testing and mainnet deployment, the PFMS core codebase is published under the Apache License 2.0, including the six engines, the stage smart contracts, the DID registry, the verification layer, the batch format and the test vectors. State specific connector configurations, signing keys and credentials remain private.

DELIVERABLE	WP	EVIDENCE TYPE
Penetration test findings fixed and retested; multi signature signer service live	WP8, WP5	Reports
Contracts and custody validator deployed to mainnet, with the policy identifier and addresses published	WP5	On chain data
All record kinds committing from live sources on mainnet	WP2, WP4	On chain data
Stage 4 and Stage 5 modules delivered and tested end to end	WP7	Reproducible test + working artifacts
100,000 transactions from live sources on mainnet	WP7	On chain data
Verification layer live and returning bundles on real records; first evidence trail documents returned from mainnet records	WP6	Working artifacts + reports
Open source release: the PFMS core codebase published under the Apache License 2.0, while state specific connector configurations, signing keys and credentials are kept private	WP8	Public repository + licence
M3 milestone report	WP8	Reports

Passed security testing, contracts on mainnet, every record kind committing from live sources and a working verification layer each stand on their own and confirm each other. The transaction hashes can be checked against the penetration test report and the tagged release, so a missing piece shows up and a report on its own cannot carry the milestone.

M4: Sustained Usage (Month 15)

M4 is assessed over a sustained mainnet usage period of three months following M3, with performance measured entirely on chain. Acceptance requires a minimum of 390,000 transactions over the period from the sources live at the time, across all five stages, with continuous daily activity throughout. This reflects the first commissionerates and districts coming onto PFMS, not the state at full adoption.

DELIVERABLE	WP	EVIDENCE TYPE
Sustained mainnet usage for three months: a minimum of 390,000 transactions from live sources across all five stages, under the batching policy published at M3	WP7	On chain data
Usage report showing what the chain records over the period: how much was committed, from which stages, from how many of the registered sources, and how steadily it arrived	WP8	On chain data + reports
Guide to testing a record	WP1	Working artifacts
Final open source handover: the final tagged production release, technical documentation, deployment guides, reproducible tests and all five stage modules in the public repository	WP7, WP8	Public repository + tagged release + licence + reproducible build and test documentation
M4 milestone report	WP8	Reports

The whole period sits on Cardano mainnet under published policy identifiers.



How acceptance works

Every deliverable carries at least one of four evidence types: on chain data, working artifact, reproducible test, or report. Each milestone is accepted on several of these together. A report has to match the tagged release it describes, and both have to match what Cardano shows, so a milestone cannot be passed on paperwork alone and cannot fail because one document is missing.

On chain evidence is addresses, transaction hashes, policy identifiers and counts. Where a table says preprod it means preprod, and where it does not it means Cardano mainnet. Modules are proven on preprod through M2 and on mainnet from M3, after penetration testing has passed. No real record is committed to mainnet before penetration testing of the contracts it lands on, with every finding fixed and retested. Working artifacts are tagged releases, specifications and test vectors. Reproducible tests are documented procedures that give the same result every time they are run, and are demonstrated at each milestone review.

No source record is exposed in acceptance evidence. Records stay in their system of record. What acceptance works on is fingerprints, summarised strings of hashes, proofs, commit references, transaction hashes and counts. That is the same rule the system itself holds to: the fingerprint travels, the file does not.

Proving volume and operating volume are different things. The 100,000 mainnet transactions at M3 are produced by records captured from live sources through the deployed contracts. The figures in Section 4.3.2 are projections of operating volume after launch.

7. Governance and Withdrawal Management

We meet the requirements of the Cardano Constitution, as follows:

Article II §6 Governance action standards and immutable document

This proposal is submitted in a standardised, legible format containing a title, abstract, rationale, budget, milestones and supporting material, with a URL and hash of all off chain content. The signed CIP-100/108 anchor metadata is pinned to IPFS, and its CID is the on chain anchor providing the immutable reference. The metadata embeds the blake2b-256 hash of this proposal document, so the chain from on chain anchor to IPFS metadata to document allows any served copy to be byte verified against the immutable record regardless of where it is hosted.

Article II §7.1 Terms of the withdrawal

The purpose of the withdrawal, the 15 month delivery period and the costs and expenses of the proposed activities are set out in Section 6. The withdrawal is fixed at 9,600,000 ADA, and project expenditure is hard capped at USD 0.30 per ADA, which is USD 2,880,000. Any value above that cap is returned to the Cardano Treasury. We commit to returning Treasury ADA in four circumstances:

- 1 **Unspent ADA at programme end.** Any funds not spent are returned to the Cardano Treasury according to the final published reconciliation.
- 2 **Material milestone failure.** Where a milestone is not delivered and not remediated, undisbursed tranches are not released.
- 3 **Fraud.**
- 4 **Scope abandonment.**

A final reconciliation is published as part of the oversight reporting cycle.

Article II §7.2 24 month prior receipt disclosure

Trivolve Tech and Quixy (Vivid Minds Pvt Ltd) have not received ADA from the Cardano Treasury through a Treasury Withdrawal Action under Article II §7 in the prior 24 months. Separately, we disclose our Project Catalyst funding history: six community funded engagements across Fund 12 and Fund 14. These community funded engagements total ~1.49M ADA of Catalyst work to date, with 5 completed, and 1 in active delivery.

Article II §7.3 Within the Net Change Limit

The 9,600,000 ADA requested sits within the ratified 500,000,000 ADA Net Change Limit covering Epoch 613 to Epoch 713, both on its own and in aggregate at the time of submission.

Article II §7.4 Audit and oversight metrics allocation

An Admin and Audit allocation is included in the budget, covering the Cardano Foundation's administration costs (which also covers necessary taxes and expenses) and the costs of competitively procured independent third-party assurer. The assurer will review the quality of the delivered work and also conduct independent audits. Procurement will begin as soon as the first tranche is released, with the procurement published, and audit reviews at M1, M2, M3 and M4 in line with the milestone gated disbursement schedule. The same allocation funds the oversight metrics on the use of the ADA.



7. GOVERNANCE AND WITHDRAWAL MANAGEMENT · CONTINUED

Article II §7.5 Named administrator

The Cardano Foundation is the named administrator of this proposal.

Article II §7.6 Custody plan

Funds withdrawn under this Treasury Withdrawal Action are held by the administrator's multi-sig wallet address. The address is not staked to a Stake Pool and is delegated to the auto abstain predefined DRep. Treasury funds cannot therefore be used to influence governance votes or stake distribution while held.

Treasury Withdrawal Guardrails

GUARDRAIL	REQUIREMENT	STATUS
TREASURY-02a	Withdrawal shall not exceed the Net Change Limit for the relevant period	Compliant. Does not exceed the NCL at the moment of submission
TREASURY-03a	Withdrawal denominated in ada	Compliant. All amounts denominated in ₳. USD figures are reference only, at a planning rate of \$0.23, with expenditure capped at \$0.30 per ADA

Administration

The Cardano Foundation will serve as the constitutional administrator of this proposal. The Cardano Foundation will conclude an off-chain legal contract with Trivolve Tech for delivery in line with the commitments of this proposal.

Delivery of milestones and acceptance thereof will be visible to the Cardano Community via a dashboard for this proposal, such as at treasurywithdrawals.cardanofoundation.org. Subsequent payments, once milestones are accepted, will also be publicly visible. The Cardano Foundation will utilise a multi-sig wallet address for the receipt of funds, **addr1qys6zy04ewx8wasu3k5z4lgyknh866fptc8ps7rtfpt5mvsgpk9fmnash2j45r2k0ug5vxx3eunrjlsr6r45y33xdc7s3ujhgd**, which shall not be staked with a Stake Pool Operator and are delegated to the auto abstain predefined DRep.

All funds not disbursed by the end of the delivery period are returned to the Cardano Treasury. All amounts are denominated in ada (₳9,600,000 total ask). The total USD figure of \$2,208,000 is a planning reference based on \$0.23 per ADA.



8. Risk Management

This section describes the main risks in the PFMS programme and how we mitigate them.

8.1 Build failure risk

Delivering six engines and modules across five stages within 15 months is a substantial build. Three things reduce this risk. First, the modular architecture: the six engines are built once and shared by every stage, so each stage is a module on a common core rather than a separate system. Second, experience: this is not our first large government deployment, as we have already taken state government systems into production on Cardano mainnet. Third, staged delivery: every work package is defined by its deliverables, evidence and dependencies in Sections 6.4 and 6.5, record definitions are fixed at M1, Stages 1 to 3 are proven on preprod at M2, and nothing reaches mainnet before penetration testing at M3. Because funds are released only against verified milestones, the Treasury's exposure is limited at every stage.

RISK LEVEL **Low to Moderate**

8.2 Data Feeds

PFMS depends on access to real time data from state police systems, including CCTNS, NAFIS and PIS schemas, DVR and NVR recording systems, ANPR databases, control room voice loggers, and station diary and armoury systems. Any delay in obtaining or maintaining access to these real time data sources could delay certain aspects of PFMS deployment and operation.

This risk has been substantially mitigated because the required datafeeds from these systems have already been acquired from the state. This provides PFMS with an established data foundation and reduces reliance on negotiating access to these systems during delivery.

RISK LEVEL **Low**

8.3 Adoption

PFMS only creates value if the government uses it beyond the funded period. This risk is low because the state government is commissioning PFMS for its own daily operations. Adoption is therefore not a separate or speculative objective. It is a core requirement of the government for the solution to be deployed and used across its operations.

Running PFMS after programme completion follows the same model as our previous project, FMS. FMS was funded and delivered as a complete solution, after which the state took over its operation and has been running it on its own infrastructure for more than a year. The continued operation of FMS has resulted in more than 156,000 Cardano Mainnet transactions to date.

PFMS follows the same model. By M4, the system will already have been in sustained use on Cardano mainnet. Upon project completion, the government will deploy and operate PFMS on its own infrastructure, with our continued support. Its ongoing use across the state will generate recurring Cardano mainnet transactions, sustaining adoption beyond the funded project.



In other words, as the solution is brought into use across the participating government facilities, adoption becomes an inherent part of the system's day to day operation rather than a separate assumption.

The PFMS project agreements contain confidential state information and cannot be shared publicly. They have been reviewed by the Cardano Foundation as administrator.

RISK LEVEL **Low**

8.4 Financial Discipline

ADA price is the most visible market risk, and one we have already carried through delivery. Upon withdrawal, the ADA price risk will be professionally hedged insofar as possible to ensure cost coverage over the course of the proposal. During our Catalyst proposal for IndianChain, another Indian state government deployment, the price of ADA fell significantly while the work was under way. We delivered the committed solution with the same quality and scope that was promised.

The same principle applies to PFMS. We assure the Cardano community that, irrespective of any future decline in the price of ADA, we will continue to deliver the scope, quality and outcomes committed for the proposal.

At the same time, we recognise that the opposite scenario is possible. A significant increase in the price of ADA could result in a surplus relative to the initial budget. For this reason, project expenditure is hard capped at USD 0.30 per ADA, which is USD 2,880,000 on the 9,600,000 ADA ask, and any value above that cap is returned to the Cardano Treasury. All unspent ADA is also returned in full at the end of the project, following the publication of the final reconciliation.

Changes to the Cardano constitution or treasury process are outside our control and are carried as residual risk. The programme commits to a fixed reporting cadence throughout.

RISK LEVEL **Low**



9. Conclusion

PFMS does not simply bring millions of transactions to Cardano. It puts Cardano underneath one of the most consequential systems a government operates: the chain of evidence on which criminal justice depends.

Every record stamped by PFMS represents something that can matter in a courtroom. A piece of footage. A statement from a witness. A weapon. A forensic result. An arrest record. An exhibit sitting in an evidence room. A document filed before a judge.

Behind every one of those records is a human life.

If evidence is altered, an innocent person can lose their freedom. If genuine evidence cannot be proven genuine, a victim can be denied justice. If a chain of custody cannot be established, a guilty person can walk free. These are not theoretical consequences. They are the stakes of the system we are putting on Cardano.

This is why the scale of PFMS matters beyond transaction volume.

The system will generate millions of transactions, but the greater achievement is what those transactions represent. They demonstrate that Cardano can operate as the trust layer for a government system where complexity is at its highest, where thousands of institutions, millions of records and hundreds of thousands of people interact with the system, and where the integrity of a single record can change the course of a person's life.

This is a fundamentally different test of a blockchain.

A financial system measures failure in dollars. A supply chain measures it in delayed shipments. A government evidence system measures failure in something far more serious: justice denied, freedom taken, and lives permanently changed.

If Cardano can provide the immutable foundation for this system at state scale, it proves something far more valuable than throughput. It proves that Cardano can be trusted when the consequences of failure are human.

9.1 What it opens

A proven reference for government deployment

Governments do not adopt technology because it is elegant. They adopt it because someone comparable adopted it first and it worked.

Today, no blockchain has a state scale criminal justice deployment to point to. After PFMS, Cardano does.

That changes the conversation. The next government does not have to be shown a prototype. A ministry does not have to be asked to believe that blockchain can support its most sensitive records. A state does not have to be the first to take that risk.

There will be a live system to point to.

This is how infrastructure becomes a standard: someone has to be willing to prove it first.



A system that can repeat across India

The chain of evidence is not specific to a single state or a single country. Every state and country runs police stations, evidence rooms, forensic laboratories, prosecution offices and courts. The institutional structure changes in detail, but the fundamental problem remains.

What is built here is therefore not a one state application. It is an open source evidence layer for an entire category of government infrastructure.

India has 36 states and union territories. A successful deployment in one state creates a pathway for the other 35.

And beyond India, the same problem exists wherever criminal justice depends on records that must remain trustworthy years after they were created.

Infrastructure tested under real consequences

PFMS also gives Cardano something that benchmarks cannot.

A blockchain can demonstrate throughput in a test environment. It can demonstrate reliability under controlled conditions. PFMS asks a harder question:

Can the network remain a trustworthy foundation when the record being stamped may one day determine whether someone goes to prison, whether a victim receives justice, or whether a case collapses?

That is a different standard.

The system will exercise Cardano's identity, transaction, verification and infrastructure capabilities under real institutional conditions, across thousands of government endpoints and millions of records.

Demand that does not follow the market

Crimes do not stop because markets fall. Evidence does not stop moving because ADA is in a bear market. Courts do not stop hearing cases because sentiment changes.

The activity generated by PFMS comes from the ordinary operation of government.

Cases are registered. Evidence is collected. Exhibits move. Records are filed. Statements are produced. Documents reach courts. Evidence is called years later.

That creates a category of blockchain activity whose demand is tied to real world institutional activity rather than market cycles.

A Treasury that earns

The Treasury does not simply fund an application and move on. It funds open source infrastructure, a public good, that creates sustained network usage, establishes a government reference deployment, opens the door to further deployments in India and beyond, and returns 70% of verification revenue to the Treasury.

The funding becomes an investment in an infrastructure loop rather than a one time expenditure.



9.2 What it comes to

The ambition is not simply to put a government application on Cardano.

It is to put a system responsible for protecting the integrity of justice on Cardano, and prove that the network can carry that responsibility at scale.

Because the ultimate measure of PFMS is not the number of transactions it produces.

It is the number of times an honest police officer can prove that the record was honest.

It is the number of times a victim does not have to watch a case collapse because nobody could prove what happened to a piece of evidence.

And it is the number of times an innocent person is not asked to surrender years of their life because a record could not prove itself authentic.

Every transaction is a timestamp. Every timestamp protects a record. Every protected record protects the truth. And behind that truth is a person.

Somewhere, there is a victim waiting for justice.

Somewhere, there is an accused person waiting to know whether they will lose their freedom.

Somewhere, there is a family waiting for a court to decide what happened to someone they love.

They should not have to depend on whether a register was rewritten, whether a file was replaced, whether a recording was edited, or whether an officer can remember what happened years ago.

They should have a record that can prove itself.

That is what PFMS is being built to deliver.

And that is why this proposal is bigger than a blockchain deployment.

It is a commitment to build a system where the truth does not depend on memory, paperwork, or trust alone.

Because when justice depends on evidence, the integrity of that evidence is not a technical problem.

It is a human one.

And when a person's freedom, a victim's justice, or an entire family's future can depend on a single record, that record deserves a foundation that cannot be rewritten.

We believe Cardano can be that foundation.

PFMS is the opportunity to prove it.