1. Title

Cheat-Proof Faraday-Cage Competition Pod with Integrated Multi-Sensor Telemetry, Cryptographic Chain-of-Custody, Biometric Presence Verification, and Conditional Wager Escrow

2. Description

Field of the Invention

Secure competitive gaming environments; anti-cheating infrastructure; blockchain-backed event verification; biometric authentication; automated escrow for skill-based wagering.

4. Background

The Faraday-Pod system, occupies a unique IP niche: it is the first to integrate **physical anti-cheat barriers, layered real-time sensors, blockchain-verifiable telemetry, biometric presence verification, and automated escrow enforcement** into a unified competition platform. Prior art covers fragments of these ideas, but not their combination. With enhanced claims capturing each layer and their synergy, this specification secures broad, defensible global IP protection.

Prior Art Analysis of the Faraday-Pod Chess Anti-Cheat System

Shielded Enclosures for Cheat Prevention

One key element of the Faraday-Pod system is a **transparent, mesh-laminated Faraday-cage enclosure** that isolates players from external electronic communications. Prior art shows that using **Faraday cages or shielded rooms** to prevent illicit communication in gaming and betting environments is known. For example, a published U.S. patent application on casino gaming discloses placing players in a **sound-proof room or Faraday cage** to reduce the possibility of outside communication or signaling . Similarly, a recent U.S. patent for an avatar-based sports betting system suggests constructing a **local betting venue as a Faraday cage** so that no

wireless signals can penetrate . These references establish that **EM-shielded enclosures** for fairness in games or betting are known. However, they generally describe the concept in broad terms (isolating players or bettors to block signals) and **do not specifically teach a transparent, mesh-laminated structure** optimized for in-person board game competition. The Faraday-Pod's implementation – a *transparent cage with embedded conductive mesh* – aligns with known EMI shielding techniques (e.g. metalized transparent screens in Faraday enclosures), but applying this to a **mobile, player-sized booth for chess or e-sports** appears novel. Importantly, none of the identified prior art combines the shielding with the *full cheat-detection suite* of the Faraday-Pod. The Faraday-Pod's enclosure could therefore be claimed with emphasis on its **transparent mesh laminate construction** and its integration with sensors (mounting of cameras, antennas, etc. on the cage) – aspects not explicitly claimed in earlier patents.

Tamper-Proof Integrated Terminals

Another element is the **sealed, tamper-evident single-purpose computing terminal** inside the enclosure, used for the digital aspects of gameplay. Prior art in the casino field shows analogous concepts: for instance, Konami's security cage patent for slot machines describes a locked internal **"safety cage"** that houses critical electronics (like game logic boards or ROMs) to prevent unauthorized access or swapping . In that system, a partitioned cage inside the machine separates an **inaccessible region** (critical components secured by a lock) from an accessible region . The goal is to prevent tampering with odds or outcomes by physically restricting access to the electronics . This concept is highly relevant – it demonstrates using **physical security and locks** to ensure game integrity. The Faraday-Pod's computing terminal functions similarly: it is a dedicated chess interface that players cannot tamper with (no ability to install engine assistance, etc.), presumably sealed with tamper-evident features (breakable seals or sensors). While Konami's patent covers internal machine enclosures, it does not specifically address *human players* or external enclosures. No prior art was found that places a **tamper-proof computing device inside a Faraday-shielded booth** for human competitors. This suggests a relatively **open field** for claiming the integrated design. To strengthen IP, independent claims can emphasize that the system includes a **secured, single-purpose computing terminal** within the shielded enclosure, equipped with tamper sensors or seals that trigger alerts if breached (drawing from known tamper-detection circuits in secure devices – e.g. magnetically-triggered tamper sensors that wipe data). Dependent claims might add specifics like *how* the terminal is sealed (e.g. locked housing, epoxy potting, encryption of firmware, etc.) and how it interfaces with the external world (perhaps only via the controlled blockchain logging channel).

Real-Time Cryptographic Sensor Logging (Blockchain)

A standout feature of the Faraday-Pod is the **real-time hash-chaining of sensor telemetry and publishing to a distributed ledger (blockchain)**. This is intended to create an immutable, time-sequenced record of the environment data (e.g. cage door closed, no signal detected, etc.)

so that any tampering or lapse is evident. Prior art confirms that **tamper-evident logging via cryptographic chaining** is an established technique in other domains. A recent patent publication on secure event logging describes appending events in a chain such that logged data **"cannot be tampered, deleted, re-dated, or re-timed"** without detection . Each new event record includes a reference (e.g. hash) to the prior record, forming an immutable sequence . If an attacker alters or removes an entry, the chain's cryptographic links break, providing evidence of tampering . Another example is a U.S. patent (US 11,184,367) which applies blockchain to sensor tracking: sensors upload data to a blockchain where a **smart contract** enforces roles and logs time-stamped sensor readings securely . These concepts strongly overlap with element (3) of the Faraday-Pod. They indicate it would be wise to explicitly claim the **hash-chaining mechanism** – e.g. a system wherein each sensor reading is hashed together with the previous hash to form a chain, and periodically or continuously **publishing these hashes to a blockchain or distributed ledger** for public verification. None of the prior art found is specific to anti-cheating in games; they are generic logging or military sensor tracking systems. Thus, focusing the claims on *using blockchain-secured telemetry in a competitive gaming context* would carve out a novel niche. A dependent claim might cover variants (publishing to a public blockchain vs. a private distributed ledger, use of smart contracts to automate alerts when a break in the chain is detected, etc.). This feature significantly **strengthens enforceability** by providing clear evidence of integrity breaches – something prior systems in gaming have not combined with physical anti-cheating measures.

Continuous Biometric Presence Verification

The Faraday-Pod also proposes **biometric or motion-based verification to confirm uninterrupted human presence** throughout play. This is aimed at preventing a player from leaving the booth or being covertly replaced by another person or device mid-match. Biometric continuous authentication is a growing area of interest. In the context of online exams, for example, systems have been designed to continuously monitor the test-taker's identity and behavior. One patent application for automated exam proctoring describes taking the test-taker's photo and obtaining **voice or keystroke biometrics** to validate identity, and then monitoring audio/video feeds for anomalies . The system will flag or halt the exam if it detects that the person at the computer is not the original authorized test-taker or if they exhibit "questionable behavior" . By analogy, in a chess pod one could use a camera for facial recognition or a fingerprint sensor on the console to periodically re-verify the player's identity. Motion sensors could detect if the player leaves their chair or if an unauthorized entry into the pod occurs. Another relevant example comes from casino security: modern casinos use networks of cameras and even wearables to track players. A recent patent by a gaming company (LNW) covers deploying **multiple biometric detection devices** in a casino to track patrons' movements and verify identity (for age checks, player tracking, etc.) . This shows that **continuous identity/authentication monitoring** is known in gaming, although the goal there is regulatory compliance and personalization rather than cheat prevention.

Importantly, none of the prior references specifically address **uninterrupted presence verification in a closed match setting**. The Faraday-Pod could claim this in an independent

claim: e.g., *a system that uses one or more biometric sensors (camera, fingerprint reader, heart-beat sensor, etc.) or motion sensors to confirm that the same human player remains present and active inside the enclosure for the duration of the game*. A dependent claim might specify **motion-based tamper checks** – for instance, if the door's internal motion/light sensor detects opening (or if a pressure sensor on the seat goes inactive), the system pauses or invalidates the match. The **combination of biometric ID and physical sensors** tied into match control logic appears to be unique and not explicitly claimed elsewhere. Prior art in exams and casinos can be cited to show feasibility, but the application in a competition pod is novel. Any existing gaps (e.g., ensuring liveness detection to defeat masks or photos) could be filled with dependent claims (e.g., requiring blink detection, 3D camera for liveness, etc., to ensure it's a live person continuously present).

Wager-Escrow with Automated Anticheat Triggers

A particularly innovative aspect is the **secure wager escrow system** that releases funds only upon a clean match (i.e., no cheating detected, and the sensor/blockchain log is uninterrupted). This ties the technical cheat-detection to financial outcomes (prize money or bets). In traditional betting, there are rules to void bets in case of match irregularities, but those are usually manual and post hoc. We did not find prior patents that explicitly link *real-time cheat detection systems with an automated escrow or betting payout mechanism*. However, we can draw parallels from related domains:

- **Peer-to-peer wagering platforms** exist where funds are held in escrow smart contracts and automatically paid out to winners . For example, US9649564B2 describes an online wagering platform that places wagered funds in escrow and releases them to the winner at outcome, giving users confidence that payouts are guaranteed . This ensures the **escrow mechanism** is not novel per se.

- Some proposals for **"provably fair" gaming using blockchain** implicitly ensure that outcomes are fair before payouts occur (often by using cryptographic random seeds and verifiable results) . Those systems focus on proving the game wasn't manipulated by the house, rather than detecting player cheating, but they operate on the principle of only honoring outcomes that pass integrity checks.

- Rules in sports betting often state that if a match is annulled or a player is disqualified, bets are void – but doing this via an *automated system* tied to sensor inputs is new.

Given this landscape, the Faraday-Pod can likely claim novelty by combining **sensor-based anti-tampering verification with conditional financial transactions**. A claim could be formulated for a system where *a smart contract or escrow module holds wagered funds (or prize funds) and is programmed to release them to the designated party **only if** the match concludes without any sensor-detected tampering or chain-of-custody interruption*. If a breach is detected (e.g., the cryptographic log shows a break in sequence, or a biometric mismatch event occurs),

the system could automatically **invalidate the result and hold or refund the funds**. This "smart escrow" tied to cheat-detection triggers was not explicitly found in prior art, making it a strong point of novelty and an enforceable differentiator. Dependent claims here might cover variations such as using a **blockchain smart contract** to hold the funds versus a traditional escrow server, or triggering different actions on various types of alerts (e.g., minor alert might reduce the payout or notify an arbiter, major alert voids the match entirely).

Automated Match Lifecycle Control

The Faraday-Pod envisions that the **match lifecycle (start, continuation, end)** is governed by the sensor state transitions and their cryptographic verification. In practice, this means the system will *only start the game clock when all conditions are "green"* (both players present, door sealed, cage shield active, etc.), pause or terminate play on any integrity breach, and only finalize a result if the sensor audit trail is intact. This kind of end-to-end automation of match governance is **not present in conventional games**, which rely on human arbiters and trust. Prior art has fragments of this idea in different contexts: for example, some **online gaming platforms** enforce certain conditions automatically (an online poker system might auto-fold a player who disconnects or an e-sports system might forfeit a player who pauses too long), but those are software-level rules, not tied to physical anti-cheat hardware. We did not find patents that directly cover *physical sensor inputs driving the state of a competitive match*. The closest is perhaps ideas in the exam proctoring system, which can **suspend the exam session automatically if cheating is detected** . That is analogous: the exam ends or is paused when rule violations occur. Another related concept is the **fraud detection in casinos** where if an irregularity is detected (say extra chips appearing), the system could flag that game round – but again, final decisions are usually left to human supervisors.

This appears to be a **weakly claimed region** – an opportunity to patent the idea of *tying game state control to multi-sensor verification.* An independent claim might state: *a match control system that automatically executes state transitions (start game, end game, invalidate result) based on outputs of the integrated cheat-detection sensors and verification of their blockchain log.* This ensures that, for example, if the door sensor opens in the middle of a game (breaching the Faraday enclosure), the system might automatically pause the clock and sound an alert, preventing any secret consultation. If the blockchain log hash fails to update at the expected interval (suggesting a device malfunction or interference), the system could automatically put the match in review mode or nullify it. No prior art explicitly covers this kind of **automated referee** logic using hardware sensor feeds, so it should be emphasized as a novel and enforceable aspect of the Faraday-Pod system.

Layered Multisensor Real-Time Cheat Detection

Finally, the Faraday-Pod employs **layered multi-sensor input** – e.g. RF spectrum monitors, optical light curtains, cameras, microphones, possibly pressure mats – to detect any cheating behaviors in real time. Multisensor fusion for security is well-known generally (for instance, a

bank vault might use motion sensors + video + thermal sensors). In gaming, examples exist of using multiple sensor types to catch cheating: a classic case is the slot machine anti-cheating devices. One patent describes that modern slot machines deploy both **magnetic sensing (coin signature check) and optical sensing** (light beam break detectors) such that if a coin-on-a-string trick is attempted (coin pulled back out), the optical sensor "tilts" (shuts down) the machine . This shows a principle of using different sensor modalities to detect illicit behavior. In table games, a **casino fraud detection system** uses cameras (for chip movements) combined with game outcome data to flag discrepancies . Likewise, online exam proctoring uses *webcam video*, *microphone audio*, and even *keystroke dynamics* in tandem to detect cheating behavior (e.g., looking off-screen and hearing another voice could trigger a flag) . These all illustrate **multi-sensor approaches** to detect anomalies.

The Faraday-Pod's multisensor array is comprehensive and tailored to chess: for instance, a **light curtain** at the booth entrance could instantly detect if a hand or object crosses the boundary (preventing, say, someone passing a device to the player). An EM sensor can sniff for any electronic transmissions inside (to catch if a hidden device tries to send/receive). A camera can monitor the player's eye gaze or gestures, while a microphone might detect whispered communication or unusual noises (indicative of a hidden earpiece or device). While each of these sensors has precedents, **combining them in one integrated anti-cheating system** is novel. Prior art did not show any one system that layers **RF, optical, and audio sensors specifically to police a live competition**.

In terms of claims, this suggests adding dependent claims for specific sensor implementations: e.g., *one claim for an RF spectrum analyzer configured to detect unauthorized transmissions within the enclosure (with possibly a threshold to ignore benign signals like Wi-Fi leakage, etc.), another for an optical break-beam or LIDAR "light curtain" at the door, another for an omnidirectional microphone analyzing acoustic signatures.* Each of these can be individually novel in this context and strengthen the patent family's breadth. Notably, prior art like the slot machine light sensor or camera-based cheat detection could be cited during prosecution; however, **their scope is limited to their contexts** (slot internals or casino table management) and they do not anticipate a *portable competition pod employing all these together*. Thus, the Faraday-Pod has an opportunity to claim a **broad multi-sensor anti-cheating platform**. For enforcement, having multiple sensor types claimed also means that an imitator who omits one sensor type might still infringe other claims – a layered claim strategy can ensure coverage of various combinations (e.g., one independent claim might focus on the Faraday enclosure + computing device + blockchain logging broadly, while another focuses on the multisensor cheat-detection method inside the enclosure).

Gaps in the IP Landscape and Unclaimed Regions

Our prior art search suggests that **no single reference covers the full combination** that the Faraday-Pod Chess Anti-Cheat System proposes. There are patents in related sub-areas (EM shielding, tamper-proof hardware, blockchain logging, biometric monitoring, etc.), but the

integrated system as a whole appears unique. This means there are some *unclaimed or weakly claimed regions* in the current landscape that Faraday-Pod can occupy:

- **Integrated Physical and Digital Anti-Cheat System:** Most prior art addresses cheating either on the physical level (shielding, tamper locks) **or** on the digital level (software anti-cheat, logging). The combination – a Faraday-cage **physical environment tied to a blockchain-based digital audit trail** – is not found in patents. This integrated approach itself is an inventive concept that should be captured in claims.

- **Real-Time Automated Enforcement:** As noted, using sensor outputs in real-time to control the state of the game (pausing play, invalidating results) is not seen in prior systems which usually just *alert humans*. This is a largely unclaimed space, and adding automation logic into claims (e.g., *"wherein the system automatically halts gameplay upon detecting a breach of any sensor-verified condition"*) will cover this novel ground.

- **Conditional Wager/Payout Mechanism:** Tying cheat-detection to an automated conditional payout (escrow) is another unclaimed aspect. Competitors in the patent literature focus either on fairness of game outcomes or on payout mechanisms, but not on *voiding a wager if cheating is detected by sensors*. This is a unique value proposition of Faraday-Pod for high-stakes matches and should be emphasized.

- **Chess-Specific or Board-Game-Specific implementations:** Interestingly, we did not locate any patents specifically about **anti-cheating in chess or similar board games** using technology. The competitive chess world has faced cheating issues (wireless signals, hidden engines, etc.), but technical solutions have not been patented (to our knowledge) – most anti-cheating measures are procedural (metal detectors, arbiters). This implies a **wide-open field** for Faraday-Pod to claim methods and devices specifically aimed at in-person board game competitions. By tailoring some claims to "a system for live intellectual competitions (e.g. chess, go, poker)" the patent could secure very broad coverage in that niche, essentially pioneering a category.

Given these gaps, the Faraday-Pod team can confidently claim novelty for core aspects. To maximize **global coverage**, it will be prudent to file in major jurisdictions (US, EP, CN, etc.) citing the unique combination of features. Each jurisdiction's patent literature (we scanned U.S., PCT/EP, and CN at a high level) shows the same pattern – pieces of the puzzle exist, but not the whole. For example, Chinese patent documents we found (CN114917571A, CN115581908A) deal with casino cheating detection using imaging, but not with enclosures or blockchain. This fragmentation means Faraday-Pod's broad vision is likely novel worldwide. Care should be taken, however, to word claims in a way that they **don't read on the prior single-aspect systems** (to avoid unnecessary prior art rejections). For instance, including the Faraday cage feature in the independent claim automatically sets it apart from many prior art systems that lacked any EM shielding.

Supplemental Specifications:

- **Advanced Signal Detection:** The draft mentions EM sensors, but one missed opportunity might be specifying *particular signal-detection techniques* like **spectrum analysis with machine learning** to distinguish normal electronic noise from a hidden transmitter. If not already in the spec, consider adding that the pod can employ signal classification (to ignore innocuous emissions but flag patterns consistent with known cheating devices, for example). This could support a patentable sub-claim on using **AI-driven EM anomaly detection** within the enclosure.

- **Integration with Game State (Digital Cheat Detection):** The focus is on physical and electronic cheating, but another layer is **digital move analysis**. Chess cheating is often detected by comparing moves to engine moves. The Faraday-Pod could optionally run a chess engine in parallel to analyze the player's moves for statistical deviations (like Ken Regan's model, though that is typically post-game). Including this in the spec – e.g., *a software module that monitors the game moves for likely engine assistance* – could provide an additional patentable feature. It creates a holistic system covering both **physical signals and move-by-move pattern analysis**. If no one has patented applying real-time engine analysis in on-site play with automatic flags, this could be an entirely new claim set (though one would need to be mindful of prior art in online cheat detection algorithms). Currently, patents like US20210264736A1 (which is more about casino games) do not touch chess engine detection, so this could be a differentiator.

- **User Experience and Safety Features:** The draft understandably focuses on anti-cheat, but what about ensuring player comfort and safety in a sealed pod? Features like ventilation systems that maintain the Faraday integrity, or a one-way transparent material to reduce player stress, etc., could be mentioned. While not central to anti-cheat, if the team has innovated here (e.g., a ventilation design that won't allow signal leakage), that can be patentable as an improvement to Faraday enclosures. For instance, Apple has a patent on a shielding chamber with ventilation for device testing – in a similar vein, a **ventilated Faraday competition booth** design could be claimed.

- **Tamper-Evident Match Artifacts:** One idea: the system could produce a **cryptographic match report or token (e.g., an NFT)** after a clean match, which serves as a verifiable certificate that the game was fair. This merges the blockchain aspect with a nice feature for players/organizers (and even collectors/fans). If not in the spec, consider adding that the system outputs a digitally signed record of the match (moves, sensor log hashes, outcome) that anyone can independently verify on the ledger. This is an attractive feature for global tournaments and also **patentably distinct** (combining anti-cheat with post-match authentication). It aligns with trends of blockchain in e-sports for verification of results.

- **Calibration and Self-Test Mechanisms:** A robust system would include routines to self-check sensors (e.g., periodic test pings on the light curtain, reference signals for the EM sensor, test fingerprint readings, etc.). If the draft doesn't mention it, adding how the system self-calibrates and ensures sensors are operational throughout could be useful. It could lead to claims like *"wherein the system periodically injects test data or challenges (e.g., a test RF pulse) to verify that each sensor and the logging mechanism are functioning correctly during the match"*. This ensures that a clever cheater cannot simply jam the sensor and go undetected – because a lack of expected test acknowledgment would itself be a red flag.

- **Global Play and Remote Supervision:** Perhaps outside the immediate scope, but consider the scenario of **remote referees or audience**. The blockchain publishing already makes the data public; an extension is a feature where remote officials (or even the opposing team's coach) can monitor the live telemetry via a dashboard. The spec could mention a *remote monitoring system that receives the real-time blockchain data and sensor feeds*, giving transparency to all stakeholders. Patent-wise, this could be a dependent claim on a *monitoring server or device that in real-time verifies the chain and displays alerts if something is off*, effectively a **distributed anti-cheat alarm system**. This is another selling point for global tournaments (multiple arbiters can oversee without being physically present) and can bolster novelty (traditional anti-cheating requires on-site arbiters; this system could allow off-site supervision which is new).

In summary, the Faraday-Pod system is quite comprehensive, and our research **confirms its core novelty**: none of the identified prior art references anticipate the full combination or many of the sub-combinations. There is strong prior art in each individual area, which we have cited (e.g., Faraday enclosures , security cages , blockchain logging , biometric tracking , etc.), but these serve to show the problem has been recognized in pieces.

The Faraday-Pod's innovation is in **synthesizing these elements into an integrated solution** for competitive fairness and then pushing the envelope with features like automated escrow and match control. By capturing these nuances in the patent claims (as recommended) and possibly extending the spec to cover the "missed" ideas above, the team can secure a **strong, enforceable patent portfolio globally**. This will not only confirm the novelty over existing art but also create a high barrier for any would-be competitor trying to implement a similar anti-cheating system for tournaments.

Sources:

- Konami Corp. patent on **security cage in gaming machines** (prevents access to critical components)

- U.S. Pat. Pub. 2021/0264736 A1 – use of **Faraday cage** to isolate casino game players from communication

- U.S. Pat. 11,842,601 (2023) – sports betting system suggesting a **Faraday-cage venue** to block external signals

- U.S. Pat. Pub. 2020/0344074 A1 – **tamper-evident logging of events** in a chain so data "cannot be tampered, deleted, re-dated, or re-timed"

- U.S. Pat. 11,184,367 B2 – applying **blockchain to sensor data**, using smart contracts to log and verify sensor telemetry

- U.S. Pat. Pub. 2019/0156689 A1 – automated exam proctoring system using **biometric verification and multi-modal monitoring**, with automatic session suspension on detected anomalies

- U.S. Pat. Pub. 2004/0097285 A1 – slot machine anti-cheat device using **multiple sensors** (magnetic coin signature + optical beams) to detect cheating and trigger machine "tilt"

- U.S. Pat. 12,387,561 B2 (2025) – **casino fraud detection** system using cameras and game data to catch irregular chip movements

- LNW Gaming's biometric tracking patent – deploying **multiple facial recognition cameras** across a casino for continuous identification and authentication (demonstrates industry trend toward continuous biometric monitoring).

Cheating in competitive chess and similar games increasingly involves covert electronics, hidden communication devices, or substitution of players. Prior measures: metal detectors, webcams, or exam-style proctoring, remain vulnerable. Casino systems use sensors and cages, and blockchain logging is known in IoT, but no solution integrates **physical Faraday shielding, biometric presence verification, cryptographically chained telemetry, and conditional wagering enforcement**. There is a need for such a holistic system, particularly for high-stakes matches and retail wagering venues.

5. Summary of the Invention

The invention provides a modular, transparent Faraday-enclosure booth with an integrated tamper-evident game terminal, multi-modal sensors, real-time blockchain logging, automated referee logic, and escrow payout triggers. Together, these elements create a closed integrity loop: physical cheat prevention, cryptographic proof, and automated financial enforcement.

6. Brief Description of the Drawings

- **FIG. 1** is an exploded perspective view of a transparent Faraday-cage enclosure (10) with mesh-laminated wall panels, a seated competitor, and the sealed game terminal (18).

- **FIG. 2** is a top-down schematic of the interior sensor layout showing corner cameras (12), infrared light-curtain (20), microphone array (14), RF analyzer (16), and the tamper-evident terminal (18) relative to the player.

- **FIG. 3** is a cross-section of the sealed "monolith" terminal (18) illustrating the e-ink display (28), secure SoC (24), and tamper fuse (22) within the rigid housing.

- **FIG. 4** is a system block diagram depicting sensor buses (42) feeding a hash engine (40), a ledger gateway (44) writing to a distributed ledger (48), and an escrow module (46) that releases or voids wager funds.

- **FIG. 5** is a match-lifecycle state diagram showing automatic transitions among Setup (S0), Active (S1), Pause (S2), Void (S3), and Complete (S4) in response to integrity events.

- **FIG. 6** is a sectional view of a waveguide-beyond-cutoff ventilation duct (30) that allows airflow while preserving the enclosure's RF shielding.

- **FIG. 7** is a remote monitoring dashboard (60) displaying live game data (62), player biometrics (64), integrity status (66), and real-time betting odds (68) derived from the verified ledger feed.

- **FIG. 8** is a flowchart of the conditional escrow workflow showing stake deposit (70), integrity verification (74), normal settlement (76), and refund path on a void flag (78).

- **FIG. 9** is a sensor calibration and self-test sequence executed in Setup state, including RF baseline check (82), acoustic noise floor capture (84), camera focus verification (86), biometric liveness test (88), and a decision node (89) gating transition to Active play.

- **FIG. 10** is a post-match certificate workflow illustrating aggregation of final move data (90), Merkle-root digest construction (92), on-chain signing (94), NFT minting (96), and a QR-code output interface (98) for independent integrity verification.

7. Detailed Description (Enhanced)

7.1 Faraday Enclosure

Panels of transparent polycarbonate laminated with copper mesh (≥80 dB attenuation at 2 GHz). Provides shielding while maintaining spectator visibility. Ventilation ports include waveguide-beyond-cutoff ducts to preserve RF integrity.

7.2 Multi-Sensor Suite

- **Optical cameras (12)**: Overlapping 360° coverage with gaze tracking.
- **Light curtain (20)**: Randomized IR beams across entry plane.
- **Acoustic array (14)**: Beam-forming microphones (50 Hz–24 kHz) plus ultrasonic monitoring (40–45 kHz).
- **RF spectrum analyzer (16)**: Wideband (1 kHz–6 GHz) with ML classifier distinguishing benign vs. suspicious emissions.
- **Biometric cuff (26)**: Locking wristband with HRV, EDA, IMU sensors for continuous liveness and presence verification.
- **Seat pressure sensor**: Confirms uninterrupted occupancy.

7.3 Tamper-Evident Monolith (18)

Single-purpose ARM SoC, e-ink display, sealed aluminum housing. Contains tamper fuse (22) and lockable access; breach logs immediate “tamper event.”

7.4 Cryptographic Chain-of-Custody

Hash engine (40) concatenates sensor payloads + prior hash every second. Digests sent via ledger gateway (44) to distributed ledger (48). Smart contract validates continuity; any break is public and auditable.

7.5 Automated Lifecycle Control

States S_0–S_4 as per FIG. 5. Sensors directly drive game state: door closure → Active, anomaly → Pause, repeat anomaly or tamper → Void. Blockchain continuity is a prerequisite for transition to Complete.

7.6 Conditional Wager Escrow (46)

Funds staked pre-game enter escrow. Escrow module or smart contract releases payout only if ledger confirms unbroken telemetry chain + no tamper. Breach triggers automatic void/refund.

7.7 Extensions & Applications

- Move-analysis module for statistical engine-detection integrated with physical telemetry.
- Export of signed match certificates (NFTs) containing game moves + ledger hashes.
- Remote supervision dashboards reading live blockchain feed.
- Adaptable to other games: poker, go, e-sports.

- *in another embodiment, a plurality of pods is deployed across major metropolitan areas, each linked via the distributed-ledger feed, thereby enabling international, cheat-free tournaments. Third-party sportsbooks ingest the verified telemetry and historic match database to compute live Elo-style ratings and betting spreads for each competitor."*

8. Advantages

- First system combining **Faraday shielding, biometric presence verification, blockchain telemetry, and escrow enforcement**.
- Automated referee logic eliminates reliance on human arbiters for anomaly response.
- Transparent booth maintains spectator experience while guaranteeing signal isolation.
- Scalable to retail casino environments for high-roller wagering.

Detailed Figure Descriptions (FIGS. 1 – 10)

FIG. 1 — Exploded Perspective of Transparent Faraday-Pod Enclosure

FIG. 1 illustrates the mechanical assembly of the cheat-proof enclosure 10.

- Roof panel (1)—a polycarbonate sheet laminated with copper mesh; it carries low-glare LED lighting and completes the RF shield when fastened to the corner posts.

- Side wall panels (3)—four transparent, mesh-laminated panels that form the vertical Faraday walls. Each panel seats flush into the corner frame posts (8), which are aluminum extrusions providing ground continuity.

- Door sub-assembly (4)—includes a conductive-gasket seam and a magnetic reed switch which reports "door-closed" status to the control logic.

- Base platform (7)—a steel plate with threaded inserts; it both grounds the Faraday cage and supports the player's chair.

- Sealed game terminal (18)—bolts to the base platform and faces the seated competitor.

- Light-curtain emitter/receiver rails (20)—mounted on the inside doorframe; their IR beams interlock to form an intrusion grid.

The dashed arrows show the assembly sequence: roof (1) lowers on posts (8); walls (3) slot in; base (7) completes the conductive envelope.

FIG. 2 — Top-Down Multi-Sensor Layout

FIG. 2 presents a plan view of the enclosure interior.

- A square dashed outline marks the protected volume monitored by the sensors.
- Corner optical cameras (12)—four 4 K units in each upper corner provide overlapping 360° video coverage.
- Acoustic microphone array (14)—eight mini-mics on the mid-height rail form a beam-forming ring (dashed circle).
- RF spectrum antennae (16)—two orthogonally placed monopoles scan 1 kHz–6 GHz for illicit transmissions.
- Infra-red light-curtain field (20)—shown in dashed lines across the doorway plane; any beam break raises an anomaly flag.
- Sealed terminal (18)—centrally positioned; the grid overlay represents the play surface (e.g., 8 × 8 chessboard).
- Biometric cuff signal link (24)—diagrammed as a tablet icon; it symbolizes the secure uplink from the player's wearable sensor.

FIG. 3 — Cross-Section of Tamper-Evident "Monolith" Terminal

FIG. 3 cuts through the vertical axis of the game terminal 18.

- Outer housing (30)—a 10 kg milled-aluminum block (hatched) providing RF shielding and impact resistance.
- E-ink display module (28)—flush-mounted behind a window; renders the game UI at near-zero EMI.
- Secure system-on-chip (24)—fan-less ARM processor soldered to a rigid PCB; boots only signed firmware.

- Tamper fuse (22)—a 0-Ω trace wired between the SoC power rail and ground. Any case breach shears the trace, permanently disabling the SoC and logging a tamper event.

- Gasketed rear panel (32)—laser-welded to housing; removal would trip the fuse.

  Mounting screws at each corner pass through insulating bushings to a threaded pedestal welded to the enclosure's base platform.

FIG. 4 — System-Level Data-Flow Diagram

FIG. 4 details electronic pathways between functional blocks.

- Sensor suite (12) aggregates outputs from cameras, mics, RF analyzer, light curtain, seat sensor, and near-floor detector.

- Monolith terminal (18) contributes authenticated game-move packets and its internal tamper status.

- Biometric cuff (26) streams physiological and motion telemetry.

- All feeds enter the hash engine (40) via a high-speed back-plane 42. Each second the engine emits a SHA-3 digest H□.

- Digests pass to the ledger gateway (44), which encrypts and publishes them to a distributed ledger 48.

- A secure channel (dashed) links the ledger gateway to the escrow module (46). The module receives verified "integrity OK / fail" signals and releases or voids wager funds accordingly.

FIG. 5 — Automated Match-Lifecycle State Diagram

FIG. 5 delineates the finite-state machine governing every match.

- S_0 Setup—door closed, sensor calibration, escrow funding; transition to Active on door_closed & all-green checks.

- S_1 Active—normal gameplay with live hashing; first anomaly triggers anomaly_1 edge to Pause.

- S_2 Pause—clocks halted; system or human arbiter reviews. A cleared condition issues resume_ok back to Active; a second anomaly (anomaly_2) or elapsed timeout escalates to Void.

- S_3 Void—irreversible state reached on confirmed tamper (tamper_detected) or unresolved anomalies; wagers refunded.

- S_4 Complete—entered on game_end when the hash chain is unbroken; escrow pays winner, NFT certificate minted.

  Directional arrows label the only permissible transitions, ensuring deterministic, auditable control of play integrity.

FIG. 6 — Waveguide-Beyond-Cutoff Ventilation Duct (30)

This cross-section shows an S-shaped ventilation duct (30) embedded in a wall panel of the Faraday-pod.

- **Inlet aperture (30a)** admits room air; its width (W) is less than one-quarter of the shortest wavelength to be blocked.

- **Intermediate baffle (30b)** forces airflow through a 90 ° turn, lengthening the RF path.

- **Outlet aperture (30c)** opens into the enclosure interior.

  Because the total path length (L) is greater than the guided wavelength of 2.4 GHz Wi-Fi and higher, electromagnetic energy is attenuated by ≥ 80 dB while laminar airflow keeps the player comfortable.

FIG. 7 — Remote Monitoring & Spectator Dashboard

FIG. 7 depicts a browser-based interface (60) fed directly by the system's blockchain log.

- **Game board widget (62)** shows current moves or card state.

- **Player vitals strip (64)** streams heart-rate and stress metrics.

- **Integrity status icon (66)** turns green when the hash chain is continuous, yellow during a pause, and red if a tamper event is logged.
- **Live odds pane (68)** consumes the verified feed to update betting spreads in real time.

  The dashboard enables regulators, bettors, and fans to track both gameplay and integrity at a glance.

FIG. 8 — Conditional Escrow & Settlement Workflow

A flowchart illustrates wager handling from deposit to payout.

1. **Stake deposit node (70)** locks funds in a smart-contract escrow.
2. **Match start event (72)** signals the escrow that integrity monitoring is active.
3. **Integrity verifier (74)** polls the distributed ledger for an unbroken hash chain.
4. Upon **match completion (76)** with "integrity = true," the escrow automatically releases winnings to the victor(s).
5. If a **void flag (78)** is detected at any time, the escrow triggers a full refund to all parties.

FIG. 9 — Sensor Calibration & Self-Test Sequence

FIG. 9 outlines the Setup-state routine executed before each game.

- **Block 80**: Initialize all sensor modules.
- **Block 82**: Capture RF baseline; fail-out if unexpected emission detected.
- **Block 84**: Record acoustic noise floor for adaptive filtering.
- **Block 86**: Auto-focus cameras and verify field-of-view coverage.
- **Block 88**: Perform biometric cuff liveness ping and seat-pressure zeroing.
- **Decision node 89**: If every test passes, the system transitions to Active state; otherwise it returns to Block 80 after alerting an official.

FIG. 10 — Post-Match Integrity Certificate / NFT Generation

This data-flow diagram shows creation of a verifiable match artifact.

- **Aggregator (90)** collects final move log and the terminal hash of the sensor ledger.
- **Digest constructor (92)** forms a Merkle root representing the entire match.
- **Ledger signer (94)** submits the root to the blockchain, receiving a transaction hash.
- **NFT minting module (96)** packages the move log, integrity root, and metadata into a non-fungible token.
- **Output interface (98)** displays a QR code or download link enabling any third party to verify the certificate against on-chain records.