BGA BLOCKCHAIN GAME ALLIANCE

2026

THE IGAMING UPGRADE

HOW BLOCKCHAIN IS REWIRING THE INDUSTRY

REPORT

TABLE OF CONTENTS

FOREWORD

ULLE SKOTTLING
CEO AT DEGAMING

Today's iGaming industry is confronting a fundamental question about transparency, verifiability and efficiency. This is especially clear in the economics of regulated operations. Small deposits can carry disproportionate processing fees, cross-border settlements can tie up significant amounts of working capital, and players are asked to blindly trust centralised 'black box' systems that they cannot independently verify.

In the past, Blockchain's relationship with gambling has been defined by a crypto-casino model, where pseudonymous wallets, rapid cross-border payments and platforms were operating at the edge of traditional regulation.

But, as Section 2.3 of this report notes, the value of modern Blockchain is in making activity easier to verify, not conceal. The UK Gambling Commission (UKGC)'s research cited below outlines this lack of confidence, with only a minority of respondents believing gambling activities are 'free from manipulation'. Our Glass Vault technology rewires how the industry handles its finances and rebuilds trust. Through DeGaming's Glass Vault model, we don't ask players to trust the system. We offer bankroll-as-a-service, where every bet, payout and player incentive is executed on-chain and independently verifiable. The ambition is to make the underlying evidence more transparent and auditable for players, affiliates and regulators.

We believe that truth beats trust. This shift is particularly important at a time when the industry's trust deficit remains. Players need to feel confident that games are fair, their funds are secure and their winnings will be paid. Regulators require reliable evidence that operators are meeting their obligations. In response, operators need infrastructure that is auditable and can support global scale without introducing friction or trapping capital in inefficient processes.

INTRODUCTION

IVAN FILLETTI
CEO GamingMalta

> Malta's approach to the gaming industry reflects the need for innovation and effective regulation to develop together. As blockchain and digital assets open new possibilities for the sector, that principle remains central to building trust, supporting sustainable growth and protecting players.

This report offers an international perspective on the role blockchain could play in the next phase of iGaming. Its examination of payments, transparency and verification invites discussion about how technology can strengthen the industry's foundations. At GamingMalta, we see value in bringing regulators, operators and technology providers together to explore these opportunities responsibly.

Malta's experience demonstrates the value of engaging early. In 2018, the Malta Gaming Authority introduced its Sandbox Framework , establishing a controlled environment for licensed operators to test virtual financial assets and distributed ledger technology. This enabled the Authority to build supervisory expertise alongside practical industry experience.

Those lessons, together with targeted industry consultation, informed the MGA's Policy on the Use of Distributed Ledger Technology by Authorised Persons, introduced in 2023.

INTRODUCTION

The move from a sandbox to a more mature, streamlined, and risk-based framework shows regulation evolving through evidence and dialogue.

The principles behind this approach remain clear. Innovation must preserve player protection, safeguard player funds, meet anti-money laundering and counter-terrorist financing requirements, and uphold market integrity. A technology-neutral approach allows regulators to assess new applications on their merits against these objectives.

Digital assets can offer consumers greater choice. A properly regulated route for their use also gives players access to safeguards that may be absent in unregulated environments. This requires complementary gaming and financial oversight, with appropriately authorised crypto-asset service providers operating alongside gaming-specific protections. Malta's experience offers a valuable foundation within the EU's harmonised Markets in Crypto-Assets framework.

Beyond payments, blockchain may support more transparency, traceability and accountability. Turning that potential into lasting value will require collaboration, sound governance and continued scrutiny of both benefits and risks.

For GamingMalta, this is an opportunity to deepen knowledge exchange across our international ecosystem. I welcome this report as a contribution to that exchange and encourage readers to approach its ideas with ambition and rigour. Progress will be measured by the confidence, protection, and practical value these technologies deliver to players and the wider industry.

IVAN FILLETTI | CEO

GAMING MALTA

with the contributions of the Malta Gaming Authority

ACT I THE GOLDEN AGE AND ITS GROWING PAINS

1.1 THE GOLDEN AGE OF IGAMING

The iGaming industry has firmly established itself as a massive global economic force. By 2025, consumer-facing online gambling market estimates clustered between $85 billion and $118 billion (Annex 1). However, when accounting for the broader B2B software licensing supply chain, studios, data providers, and land-based integrations, the total global interactive betting and gaming market reached approximately $450 billion.

Looking at the broader ecosystem (which includes regulated, unregulated, and unacknowledged gambling) global wagering value hit an astonishing $5.9 trillion, creating a financial ecosystem that rivals the world's largest national economies. The audience scale is equally staggering, with roughly 1.6 billion people gambling online regularly and up to 4.2 billion participating at least once a year.

A core driver of this golden age is the industry's shift to a mobile-first ecosystem. Smartphones now function as portable casinos, with nearly 80% of all online wagers globally initiated on a mobile device.

Mobile and tablet platforms captured over 53% of the online gambling revenue share in 2025. Operators have revolutionized the user experience (UX) to make it entirely frictionless, utilizing cloud-based apps, one-tap payments via Google Pay and Apple Pay, instant Know Your Customer (KYC) verification, and biometric logins like fingerprint and facial recognition.

Content and technological innovation have fundamentally redefined the gameplay experience into a multi-billion-dollar engine. The explosion of live dealer casinos and game shows, pioneered by companies like Evolution, whose live segment alone generated €1.77 billion in 2025 to capture 29% of the entire online casino market has seamlessly blended traditional table games with augmented reality and high-production TV entertainment. Titles like Crazy Time and Lightning Roulette have acted as powerful conversion tools, pulling in demographics that traditionally ignored live casinos. Additionally, operators are aggressively funding gamification and social features to boost player lifetime value, alongside an explosion in micro-betting and esports wagering. Now valued at $14.7 billion and compounding at a massive 14.3% annual growth rate, this sector is purpose-built for younger, mobile-native audiences, with mobile platforms now driving over 70% of all betting activity.

1.2 THE PRICE OF SUCCESS : THE THREE-SECTOR ECONOMY AND THE ILLUSION OF REGULATED DOMINANCE

The defining structural development of the iGaming sector is the emergence of a highly complex "Three-Sector Economy". This structural evolution is detailed in the global report by Gaming Compliance International (GCI), which reveals a significant imbalance in the global online wagering market.

Gaming Compliance International (GCI) estimates that unregulated online gambling generated $5.9 trillion in wagering turnover, or handle, in 2025, up 4% from 2024. This figure represents the cumulative value of bets placed (not operator revenue) and includes stakes recycled repeatedly through gambling platforms.

Estimates of the regulated–unregulated revenue split differ materially. GCI estimates that unregulated activity represents 78% of online GGR, while H2 Gambling Capital estimated a considerably narrower 55% offshore versus 45% onshore split in 2024. Although its precise scale remains contested, the offshore sector clearly represents a substantial part of the global online gambling economy.

Structural Breakdown of the Three-Sector iGaming Economy

SECTOR CATEGORY	REGULATORY & OPERATIONAL STATUS	REVENUE & VOLUME SHARE	CORE PRODUCT VERTICALS
Regulated Sector	*Compliant with local frameworks; holds domestic licenses, pays local gaming taxes, and undergoes routine audits.*	Significant and expanding share of online GGR.	Licensed sportsbooks, certified online casinos, state-approved lotteries, and peer-to-peer poker.
Locally Unregulated / Offshore Sector	Operates from offshore tax havens; actively targets regional players without local licenses or compliance oversight.	Estimated at between 55% and 78%, depending on source and methodology	Offshore sportsbooks, crypto-based casinos, unregulated prediction markets, and offshore poker rooms.
Unacknowledged Sector	Gambling-like products operating in regulatory grey areas; utilizes social platforms to bypass traditional classifications.	Rapidly growing; unmeasured within traditional iGaming databases	Tokenized sweepstakes, prediction exchanges, in-game loot boxes, coin-flip mini-games, and social lotteries.

SOURCE	UNREGULATED / OFFSHORE	REGULATED /ONSHORE
GCI, 2025 estimate	78%	22%
H2 Gambling Capital, 2024	55%	45%

This structural division has created a "White Noise Marketplace." To the average consumer, the operational boundaries between regulated, unregulated, and unacknowledged platforms are completely indistinguishable. Consumers perceive a single, continuous digital interface, choosing platforms based on immediate bonuses, payout speeds, and ease of registration rather than licensing status.

This "White Noise Marketplace" is triggering aggressive, highly fragmented regulatory crackdowns globally. From Germany's crushing 5.3% turnover tax and Colombia's controversial 19% VAT on deposits, to Brazil’s incoming 18% GGR tax and 15% withholding fees, the fiscal perimeter is tightening. However, these traditional enforcement mechanisms (relying on ISP blocking, local land-based mandates, and advertising bans) are failing to contain the digital grey market. Instead, they are decimating regulated Net Gaming Revenue (NGR) margins and inadvertently accelerating player flight to cheaper, offshore alternatives.

As traditional legal decrees and legacy banking walls prove obsolete against borderless digital supply, the industry faces an existential ultimatum: continue fighting an unenforceable regulatory war, or pivot to a new technological paradigm. It is this exact operational friction that is turning the blockchain narrative on its head, shifting it from a tool for offshore concealment into the ultimate enterprise framework for automated compliance and verification.

1.3 FRICTIONS OF AN AGING INFRASTRUCTURE

While iGaming front-ends have modernized into hyper-personalized, mobile-first environments, the underlying operational infrastructure remains tethered to a legacy stack. This disconnect creates severe operational and financial friction across three core pillars: treasury, identity, and core gaming logic.

a) The Treasury Layer: Capital Inefficiencies and Micro-Deposit Fees

Legacy fiat payment processing remains highly fragmented, dependent on complex networks of acquiring banks, local card schemes, and regional clearing gateways. For international operators, this architecture creates severe friction:

The Micro-Deposit Tax: The casualization of iGaming has driven a massive influx of low-velocity players making small deposits, supported by market data showing that casual games jumped from representing 5 to 7 percent of the market in 2020 to 15 to 25 percent in 2025. However, traditional credit card gateways fundamentally break on these flat-rate payment fees. A standard gateway transaction charges a percentage commission plus a fixed flat fee (e.g., $0.30). On a $5 player deposit, that flat $0.30 fee alone instantly cannibalizes 6% of the volume before factoring in processor markups, regional 3-D Secure compliance costs, or hidden FX spreads. This forces operators to mandate artificially high deposit minimums, severely damaging player conversion in their fastest-growing demographic.

Settlement Drag and FX Leakage: Cross-border settlements incur intermediary frictions that slice 1.5% to 3.5% off net revenues through adverse currency conversion rates. Furthermore, these fiat proceeds routinely settle on a T+2 or T+3 business-day delay, while international transfers can stretch to a week. This traps massive amounts of working capital in rolling banking reserves, preventing efficient liquidity deployment.

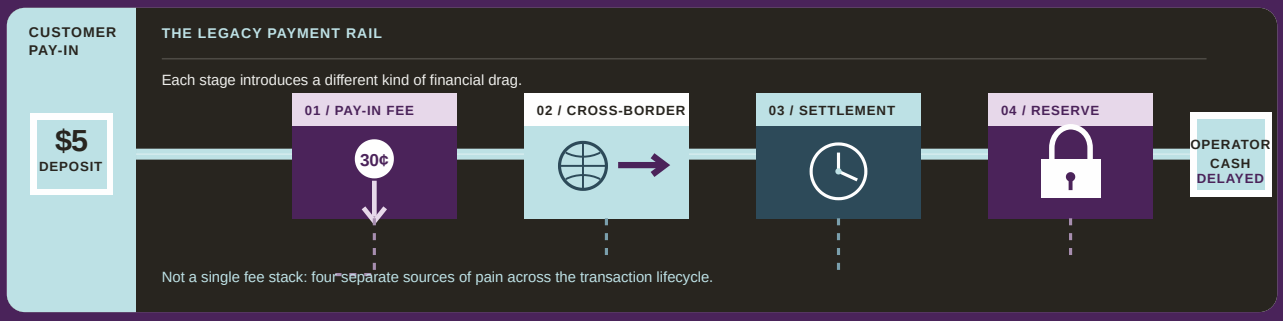
Compounding this friction, regulatory bodies demand that operators maintain immense, idle capital reserves (often matching 100% of player balances) to prove financial stability and guarantee payouts during economic fluctuations. This creates a severe liquidity trap: Regulators commonly require operators to segregate and maintain sufficient liquid assets to cover player liabilities. These safeguards restrict the use of player funds as ordinary working capital, although the assets are not necessarily idle: depending on the jurisdiction and safeguarding structure, they may be held in interest-bearing accounts or approved short-term liquid instruments. The operational burden therefore lies less in the absence of yield than in maintaining continuous liquidity, segregation, reconciliation and rapid access to funds.

b) The Identity Layer: The Asymmetric War Against Automated Fraud

Traditional Know Your Customer (KYC) workflows operate on a highly redundant, platform-centric paradigm: operators collect documents, run isolated liveness checks, assess risk, and completely repeat the entire sequence whenever a player registers on a different platform, brand, or jurisdiction. This siloed architecture assumes that an identity is a static asset to be verified from scratch at every touchpoint. While this model was sufficient for basic document matching, it represents a fundamental structural vulnerability in an environment dominated by automation and generative AI.

The Duplication Exploit: Because identity data is trapped within isolated operator databases, fraudsters exploit the lack of cross-platform attribution. A single malicious actor can combine fabricated documents, synthetic face imagery, and automated account-creation bots to move through registration flows at an industrialized scale. Treating identity as an easily replicable, independent registration artifact allows syndicates to operate massive, coordinated bot networks simultaneously across the industry.

The Onboarding Attack Velocity: According to identity network data from LexisNexis Risk Solutions, iGaming onboarding carries the highest fraud risk profile of any digital industry worldwide, with nearly 1 in every 5 new desktop account creations (20%) constituting an active attack.



The Promotional Bleed: Enabled by this systemic vulnerability, bonus abuse now accounts for a staggering 63.8% of all recorded iGaming fraud. This creates an unsustainable drain on corporate budgets, with automated promotional exploitation and multi-accounting costing a third of all global operators between 10% and 20% of their annual revenue.

Because card networks classify real-money gambling platforms as high-risk merchants, operators face zero-tolerance chargeback thresholds. Breaching a strict 1% card-scheme dispute ratio triggers immediate compliance penalties, escalating transaction processing fees, or total merchant account termination.

With cross-border iGaming fraud rates doubling globally, operators face severe financial damage. Operational audits reveal that for every $1 lost to fraudulent chargebacks, an operator absorbs an actual economic loss of $2.07 once arbitrary banking network dispute fees ($20 to $100 per occurrence), manual remediation labor, and distorted Customer Acquisition Costs (CAC) are accounted for. Operators are caught in an operational vice: lower their security barriers and face catastrophic processing bans, or tighten legacy rules and suffer devastating player abandonment rates.

The Liquidity Burden and Capital Lock-Ups : Before an operator even begins processing player wagers, they face a staggering barrier to entry regarding capital liquidity. While the industry boasts massive Gross Gaming Revenue (GGR), the reality of an operator's balance sheet is much tighter. A healthy operator's actual Net Gaming Revenue (NGR) typically hovers between 40% and 60% of their GGR once taxes, game provider royalties, bonuses, and operational costs are deducted.

However, even that remaining working capital is severely restricted by legacy infrastructure. Because traditional financial institutions classify iGaming as high-risk, payment processors enforce strict "rolling reserves". These agreements typically mandate that 5% to 15% of all daily transaction volume is locked away in non-interest-bearing accounts for 90 to 180 days to cushion against chargebacks and disputes.

The current compliance stack faces an existential crisis: it generates severe customer onboarding friction and drives up Cost Per Verification (CPV) expenditures without delivering proportionate security assurance. The critical operational challenge is no longer about deploying heavier, high-friction point solutions; it is whether the industry must completely redesign the concept of digital identity, shifting from vulnerable, single-use documentation toward cryptographically verifiable, reusable credentials.

c) The Logic Layer: The Centralized RNG "Black Box"

The foundational driver of iGaming (player trust) is handled via a highly centralized model. Game logic, Return to Player (RTP) percentages, and Random Number Generators (RNG) sit inside closed, proprietary servers audited only periodically by third-party testing houses.

To a highly skeptical, digitally native generation of players, this centralized structure is perceived as an un-auditable "black box." Because players cannot independently verify the mathematical integrity of a spin or a wager in real time, any prolonged losing streak fuels narratives of platform manipulation. This lack of cryptographic transparency severely harms long-term player retention and limits organic brand trust.

1.4 THE CRYPTO SHADOW : WEAPONIZING THE DECENTRALIZED RAIL

Squeezed between archaic fiat banking layers and crushing regulatory frameworks, a massive segment of the global market has fled to the unregulated offshore sector. It is within this shadow economy that blockchain technology found its first major iGaming use case; not as an enterprise compliance framework, but as an aggressive tool for operational evasion.

While regulated operators were suffocating under 6% micro-deposit fees, rolling banking reserves, and T+3 settlement delays, offshore platforms realized that early Web3 architecture offered a parallel financial universe. By integrating crypto-assets and stablecoins (such as USDT on high-throughput networks like Tron), the unregulated sector unlocked instant, borderless, and virtually free liquidity. They eliminated the middleman, bypassed the legacy treasury bottleneck entirely, and offered players instant payouts that traditional banking rails could never match.

However, this technological leap came with a dark trade-off. The shadow economy weaponized the decentralized rail primarily for pseudonymity. Early crypto-casinos used the technology to obfuscate player flows, bypass regional geofences, and ignore KYC compliance altogether.
This historic pairing created a profound structural paradox:

The Efficiency Proof: The offshore market successfully proved that blockchain infrastructure is fundamentally superior for global gaming scale, transactional velocity, and cost efficiency.

The Stigma Stumbling Block : By using this infrastructure to evade oversight, they cemented blockchain technology in the minds of global regulators as an inherent threat to consumer safety and financial integrity.

The industry is now left with a profound historical irony. The very technology birthed to hide shadow operations possesses the exact cryptographic transparency, immutability, and automation required to solve the regulated market's infrastructure crisis. The challenge is no longer about proving the efficiency of the tech rail; it is about rescuing it from the shadow economy and repurposing it as the ultimate enterprise framework for automated compliance and absolute player trust.

ACT II THE EVOLUTION OF BLOCKCHAIN

2.1 THE END OF THE CRYPTO CASINO ERA

The anonymous, offshore crypto casino model is rapidly approaching a regulatory and security dead end. While the initial wave of cryptocurrency gambling platforms successfully capitalized on the novelty of digital assets, their foundational architecture is no longer sustainable for the future of the iGaming industry.

The early value proposition: Payments, anonymity, and borderless gambling

Years before regulated operators showed genuine interest in blockchain technology, early crypto casinos captured market share by solving immediate pain points in traditional banking. Their core value proposition revolved around frictionless payments: Bitcoin deposits, instant withdrawals that bypassed intermediary clearinghouses, global accessibility, and strict pseudonymity.

For these early platforms, avoiding banking restrictions was the primary goal, meaning that vital institutional frameworks (such as regulatory compliance, auditability, player identity verification, and robust treasury management) were largely ignored.

However, this model of unverified, borderless gambling is no longer viable. Today, the global regulatory landscape has crystallized around strict licensing regimes and Anti-Money Laundering (AML) controls. Major offshore jurisdictions are enforcing rigorous compliance; for instance, the reformed Curaçao Gaming Authority (CGA) now mandates strict Know Your Customer (KYC) identity checks and source-of-funds controls.

Similarly, operators holding licenses in jurisdictions like Anjouan are legally required to deploy strict geo-IP blocking to restrict players from highly regulated markets like the US and the UK. Consequently, while the independent offshore sector continues to capture 78% of global Gross Gaming Revenue, the operational model of the completely anonymous, zero-KYC crypto casino is becoming severely restricted. To protect their immense market liquidity, these platforms are being forced to pivot, abandoning the evasion tactics of early Web3 in favor of enterprise-grade verification frameworks to comply with reforming jurisdictions like Curaçao and Anjouan.

The illusion of decentralization: Trust was still based on the operator

Despite heavy marketing around "provably fair" gaming, early crypto casinos rarely integrated blockchain technology into their entire operational stack. Instead, blockchain was utilized merely as a payment rail and a niche feature for RNG (Random Number Generator) verification. While platforms allowed players to verify the randomness of proprietary games using cryptographic hashes (combining a server seed, client seed, and nonce), this transparency was typically limited to a few in-house "Originals".

In reality, the vast majority of these platforms operate as "hybrid" casinos. While deposits and withdrawals utilize cryptocurrency, the rest of the gaming infrastructure remains entirely centralized. Game logic, player identity, licensing, compliance, and risk management are all handled off-chain. Crucially, this architecture is fully custodial. Players are required to deposit their funds into a casino-controlled wallet, forcing them to relinquish custody of their assets and rely completely on the operator's solvency and integrity.

Because these traditional crypto casinos store player balances and sensitive data in centralized databases, they remain vulnerable to the exact same security breaches, payment fraud, and insolvency risks as traditional fiat platforms. Ultimately, blockchain was deployed as a feature rather than true infrastructure. Moving forward, the industry's survival depends on a structural shift toward "compliance-by-design," embedding secure treasury architectures and regulatory guardrails directly into the platform's core code.

2.2 INSTITUTIONAL CLARITY ARRIVES

For much of the first crypto-casino era, digital assets existed in a legal fog. Operators could use Bitcoin, stablecoins and self-hosted wallets to move value rapidly across borders, but the surrounding questions were unresolved: Who was responsible for redemption? What reserves backed a stablecoin? Which entity was accountable for custody? Could a payment be frozen following a lawful order? And what obligations applied to an intermediary handling crypto on behalf of players?

That ambiguity was not a minor legal inconvenience. It was one of the reasons why established gaming operators, banks, payment providers and regulators treated blockchain infrastructure with caution. A payment rail may be technically fast and inexpensive, but it cannot become part of a regulated gambling stack if its issuer, reserve structure, compliance controls and legal responsibilities are unclear.

That context is changing. Across major jurisdictions, regulators are increasingly separating useful digital-asset infrastructure from the speculative and opaque practices that defined early crypto markets. The result is not a deregulated future for iGaming. It is the emergence of clearer rules for the entities that issue, custody, exchange and settle digital value.

In the European Union, the Markets in Crypto-Assets Regulation **(MiCA)** brought rules for asset-referenced tokens and e-money tokens into application from June 2024, followed by the framework for crypto-asset service providers from December 2024. In practical terms, this moves stablecoin activity away from informal issuer promises and toward authorised entities, governed reserve arrangements, redemption obligations and supervised service providers. For an operator or supplier considering blockchain-enabled payments, the question becomes less abstract: which issuer is regulated, which service provider is authorised, where are the assets held, and what protections exist if something goes wrong?

The United States has moved in a similar direction. The **GENIUS Act**, signed into law in July 2025, established a federal framework for payment stablecoins. Its central logic is straightforward: a stablecoin intended to function as money-like infrastructure must be issued by an eligible entity, backed by reserves and subject to financial-crime controls. The framework also recognises that payment stablecoins cannot operate outside the reach of law enforcement, requiring issuers to maintain the capability to comply with lawful orders where applicable.

This is a significant change in the institutional perception of digital assets. Stablecoins are no longer discussed only as speculative instruments or as tools for bypassing banks. Under emerging frameworks, they are increasingly treated as regulated payment infrastructure: instruments that may be programmable and globally transferable, but that must also be backed, redeemable, accountable and controllable within a defined legal perimeter.

Our Stablecoins & Gaming report describes this shift as the emergence of an international regulatory baseline. MiCA in Europe, the GENIUS Act in the United States, and related developments in jurisdictions such as Singapore, Japan and Hong Kong all point toward a common direction of travel: reserve backing, regulated issuance, transparency, redemption rights and stronger oversight of intermediaries. The details differ by jurisdiction, but the strategic signal is consistent. Digital assets are being pulled into the financial system rather than left outside it.

While stablecoins achieved statutory legitimacy under the GENIUS Act, broader U.S. crypto market structure suffered a major setback on September 15, 2026, when the Senate failed to advance the CLARITY Act. This creates a split regulatory reality: payment stablecoins now operate as federally recognized, reserve-backed payment infrastructure, but custom gaming tokens, decentralized platforms, and digital commodity exchanges remain without a unified federal framework. Consequently, U.S.-facing iGaming operators cannot rely on a single statutory rulebook for broader Web3 mechanics, leaving on-chain gaming logic exposed to agency-level enforcement actions and evolving court interpretations.

For iGaming, this matters because the industry does not need another unregulated payment option. It needs payment and treasury infrastructure that can withstand scrutiny from regulators, banks, auditors, payment partners and players. A regulated stablecoin issuer or authorised crypto-asset service provider may offer a more legible counterparty than the fragmented, offshore structures that characterised the first generation of crypto gambling. It creates a basis for assessing reserve quality, redemption mechanisms, sanctions controls, custody arrangements and transaction-monitoring responsibilities before an operator ever exposes a player to the rail.

However, institutional clarity around digital assets must not be confused with clarity around gambling itself.

MiCA does not grant an online gambling licence in Europe. The GENIUS Act does not authorise a casino or sportsbook to accept stablecoins in the United States. A compliant stablecoin does not override national gambling laws, local tax rules, responsible-gambling obligations, source-of-funds requirements, game certification standards or market-specific restrictions on payment methods. The gambling licence remains the centre of gravity. Digital-asset regulation simply makes one component of the operating stack more governable.

This distinction is strategically important. It prevents the industry from repeating the mistakes of the crypto-casino era, where technical possibility was often mistaken for regulatory permission. The question is no longer whether a player can technically deposit a stablecoin from anywhere in the world. The question is whether a licensed operator can use a regulated digital-asset rail within its permitted markets while preserving KYC, AML, player-protection, geolocation, auditability and financial safeguards.
That is the real significance of institutional clarity. It gives regulated iGaming businesses a path to evaluate blockchain not as an escape route from the rules, but as infrastructure that can increasingly operate inside them.

This does not mean the transition is complete. Supervisory practices are still developing, national implementations vary, and the interaction between digital-asset rules and gambling regulation remains highly jurisdiction-specific. But the direction is now materially different from the early days of crypto gambling: the industry is no longer choosing between innovation and compliance. It is beginning to explore whether innovation can become a more credible mechanism for compliance itself.

2.3 A TOOL FOR VERIFICATION, NOT CONCEALMENT

Institutional clarity changes the strategic question facing blockchain in iGaming. The issue is no longer whether the technology can move value outside conventional financial systems. The first generation of crypto casinos demonstrated that years ago. The relevant question for the regulated industry is different: can distributed infrastructure help operators, suppliers, regulators and players verify that critical systems are functioning as intended?

This represents a fundamental change in purpose.

We've seen above that in its earliest iGaming applications, blockchain was commonly associated with pseudonymous wallets, borderless deposits, rapid withdrawals and the ability to operate beyond the reach of traditional banking and licensing structures. In this model, decentralised rails were often used to minimise visibility. They made it easier to move funds across borders, but they did not necessarily make an operator more accountable to its players, regulators or commercial partners.

The emerging enterprise model reverses that logic. Blockchain's value lies not in hiding activity, but in creating durable, cryptographically verifiable records of the activities that matter most: deposits, withdrawals, game outcomes, player liabilities, responsible-gaming limits, identity checks, software updates and compliance decisions. The ambition is not to make gambling more opaque or less regulated. It is to make the underlying evidence more reliable, more accessible to authorised parties and harder to alter after the fact.

This is not yet a story of every major operator moving its core wagering stack on-chain. Public evidence does not support such a claim. Large regulated operators remain cautious, rightly so, given the complexity of licensing, data protection, game certification, payments and legacy integrations.

The more meaningful early signal comes from the suppliers that build and certify the industry's infrastructure.

IGT, for example, has protected intellectual property relating to blockchain-based responsible-gaming systems, including models in which relevant wagering limits and player-protection information can be securely shared across participating properties. It has also filed patents for digital lottery ticketing architectures based on signed records and transaction certification. Aristocrat has similarly protected distributed-ledger approaches for ticketing and for confirming that certified software has been installed on gaming devices. These patents should not be presented as evidence of market-wide deployment. They are, however, strategic indicators: established gaming technology groups are exploring distributed ledgers where the industry has its greatest need for proof, traceability and controlled data sharing.

The same logic is already visible in the wider sports-betting integrity ecosystem. Data and integrity providers such as Sportradar, Genius Sports and the International Betting Integrity Association have built commercial models around monitoring, anomaly detection, information sharing and evidence-based investigation. Their services reflect an established market reality: trust in betting cannot depend solely on an operator's internal assertion that its systems are fair, its data is accurate or its controls are effective. It increasingly depends on the ability to produce evidence.

Distributed ledgers do not replace integrity monitoring, independent testing laboratories or regulatory oversight. They can strengthen the evidentiary layer beneath them. A well-designed ledger can establish when an event was recorded, who authorised it, whether it was altered and which parties validated it. In practical terms, this can create a more reliable audit trail between the data source, the operator, the game provider, the payment provider and the regulator.

The strategic importance of this shift is reinforced by the industry's persistent trust deficit. Consumer research from the UK Gambling Commission shows that confidence in core aspects of gambling remains incomplete: only a minority of respondents strongly believe that games are regularly tested for fairness, that gambling activities are free from manipulation, or that advertised odds accurately reflect the likelihood of winning.

These findings do not prove a direct percentage of player churn caused by opacity; no sufficiently robust public dataset supports that precise causal claim. But they reveal a commercial vulnerability. In an industry dependent on repeat participation, even a small erosion of confidence can weaken retention, increase disputes and make licensed operators less competitive against simpler, faster and less accountable offshore alternatives.

The value proposition is therefore not that blockchain automatically increases Gross Gaming Revenue. Its contribution is more fundamental and more defensible. It can help protect the conditions under which sustainable revenue is generated: player confidence, regulatory credibility, operational resilience and the ability to demonstrate compliance without relying exclusively on manual reporting or retrospective audits.

This point is well illustrated by the perspective of **Ulle Skottling, CEO of DeGaming**. Speaking to the Blockchain Game Alliance, Skottling argued that the critical opportunity is not merely to accelerate withdrawals, but to make the operational state of a casino more visible. In his model, players should be able to see that funds exist in the bankroll, understand how liabilities evolve as players win or lose, and observe the consistency with which major withdrawals are processed. The objective is not to expose every commercial detail, but to reduce uncertainty around the issues that matter most to players: whether the operator can pay, whether funds are properly managed and whether a delayed withdrawal reflects a legitimate control or an unexplained failure.

As he puts it, “the purpose of the blockchain is not to keep things anonymous… it’s the purpose to keep check on things.” This is a vendor perspective rather than independent market evidence, and it should be treated as such. Yet it captures the broader transition underway: blockchain is increasingly relevant not because it enables anonymous gambling, but because it can support verifiable solvency, traceable financial flows and evidence-led compliance.

This enterprise approach must remain clearly separated from the shadow-crypto model described in Act I.

Permissioned Blockchain does not require a public ledger containing raw player data, unrestricted participation, speculative token exposure or anonymous access. It can be built on permissioned or hybrid networks in which validators are known legal entities, access rights are governed, sensitive data is encrypted or held off-chain, and regulators or auditors have defined verification rights. In this model, cryptography is used to minimise unnecessary disclosure while preserving the ability of authorised parties to verify a claim.

Zero-knowledge proofs are particularly important to this distinction. They can allow a player or counterparty to demonstrate that a required condition is true, such as being over the legal age, passing a KYC check or being eligible to participate in a specific jurisdiction, without exposing the underlying personal information to every party in the process. The compliance signal is preserved; the unnecessary data exposure is removed. Something we will focus on in section 3.4 around Identify Verification.

Blockchain alone does not make an operation truthful. A ledger can prove that a record has not been changed after it was entered; it cannot guarantee that incorrect data was never entered in the first place. Any credible deployment must therefore combine the technology with trusted data sources, clear governance, independent audits, robust identity controls and meaningful regulatory access.

The strategic shift is nonetheless clear. The future role of blockchain in iGaming is not to replace regulation, nor to recreate the anonymity of the offshore crypto-casino era. It is to provide a stronger verification layer for an industry in which payments, compliance, game logic and player trust are increasingly inseparable.

The following chapters move from this macro thesis to practical execution: how verifiable game logic can address fairness concerns; how stablecoin rails can improve treasury and settlement; and how auditable compliance and privacy-preserving identity systems can reduce risk without creating unnecessary friction.

ACT III THE BRIDGE: SOLVING THE FRICTIONS

3.1 RESTORING PLAYER TRUST (VERIFIABLE FAIRNESS & ESCROW)

For years, the industry's answer to "is this game rigged?" was a black box: a closed RNG players were simply asked to trust. As we mentioned above, the crypto-casino world produced a partial fix; "provably fair" systems where a player can recompute each round from a set of cryptographic seeds. Platforms provided tools where a player could manually input a client seed, revealed server seed, and nonce to verify a given round.

However, this architecture remains structurally flawed. The verification happens after the bet, round by round; it still depends on the operator revealing the honest seed.

More importantly, a cryptographic seed is commercially irrelevant if the platform’s treasury is centralized and custodial. Proving a spin was fair does nothing to restore player trust if the operator can arbitrarily lock an account or delay a withdrawal request.

To permanently resolve this trust deficit, operators must shift from manual seed verification to automated, on-chain execution. This is achieved through two synchronized decentralized technologies :

Escrow Smart Contracts

A neutral on-chain contract locks the player's wager and the casino's payout reserve before gameplay. Once the result is confirmed, settlement executes automatically.

Decentralized Oracles (ChainLink VRF)

Verifiable randomness is delivered on-chain through a tamper-resistant oracle network, helping ensure the outcome cannot be manipulated by the house.

This framework (decentralized oracles) is now institutionally validated; BMM Testlabs has officially granted Chainlink VRF the GLI-19 compliance certification. Marking the first compliance certification in the blockchain industry, this regulatory milestone allows licensed iGaming applications to confidently deploy Chainlink VRF as a verifiable, tamper-proof RNG that satisfies strict jurisdictional requirements.

Under this model, the outcome is mathematically guaranteed to be unbiased, and the payout is instantly routed to a non-custodial wallet without human intervention. The smart contract acts as the ultimate guarantor, entirely eliminating counterparty risk at the individual game level.

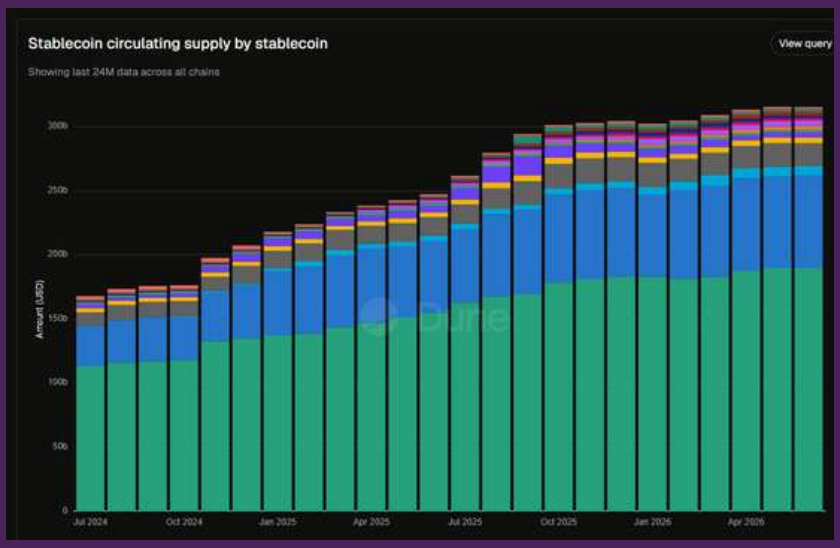
3.2 REWIRING THE PAYMENT AND TREASURY LAYER

As established in Act I, the iGaming industry's legacy treasury layer is suffocating under micro-deposit fees, rolling banking reserves, and multi-day settlement delays. Traditional fiat rails were simply not built for the instant, borderless, and high-velocity demands of modern digital economies.

Stablecoins offer the structural rewiring necessary to fix this friction, acting as a price-stable, programmable bridge between digital engagement and real-world utility.

The Weight of the Ecosystem: A Mature Global Infrastructure

The stablecoin ecosystem is not a niche or speculative experiment; it is a massive macroeconomic force. To understand the reliability of this solution, one only needs to look at the circulating supply and transaction velocity. By early 2026, the global stablecoin market capitalization exceeded $318 billion.



This immense scale builds on a trajectory that was already undeniable in 2024, when the combined 30-day transaction volume for major stablecoins like USDT, USDC, and DAI reached $1.369 trillion, surpassing Visa's monthly average.

For that full year, total stablecoin transfer volume hit an astonishing $27.6 trillion, effectively exceeding the combined transaction volumes of traditional giants like Visa and Mastercard. This mature, highly liquid infrastructure provides iGaming operators with a battle-tested, enterprise-grade foundation.

The Structural Shift: Traditional Fiat Rails vs. Stablecoin Rails

To visualize why stablecoins represent an infrastructural paradigm shift rather than just a marginal improvement, we can compare the underlying mechanics of traditional fiat settlement against blockchain-native payment rails:

Operational Metric	*Traditional Fiat Rails (The Act I Bottleneck)*	*Stablecoin Architecture (The Solution)*
Settlement Velocity	**T+1 to T+3 business days**; heavily bound by banking hours, weekends, and clearing house processing windows.	**Instant (Seconds/Minutes)**; near-real-time settlement operating 24/7/365 independent of traditional banking calendars.
Transaction Unit Economics	**High percentage** (1.5%–3.5%) + heavy flat fees ($0.30+) per transaction. Aggressively penalizes micro-deposits.	**Fractions of a percent** (<1%) driven by predictable network gas fees, entirely bypassing traditional card interchange networks.
Cross-Border & FX Friction	**High-friction and multi-layered**; involves multiple intermediary/correspondent banks with aggressive FX markups (2%–5%).	**Borderless by default**; native peer-to-peer routing with near-zero geographical or jurisdictional friction.
Chargeback & Fraud Risk	**Severe exposure**; friendly fraud and chargeback disputes can pull capital out of accounts up to 120 days post-transaction.	**Zero chargeback risk**; absolute cryptographic transaction finality. Transactions are immutable once recorded on-chain.

Operational Metric	*Traditional Fiat Rails (The Act I Bottleneck)*	*Stablecoin Architecture (The Solution)*
System Automation	**Siloed and fragmented;** reliant on batch-processed banking files, legacy API wrappers, and manual accounting reconciliation.	**Fully programmable;** native smart contract composability allows automated revenue splits and programmatic treasury flows.
Capital Efficiency	**Low productivity**; payment processors require rolling reserves (typically 5%–10% of volume locked for 90+ days) to cover risk.	**Maximum productivity**; no rolling reserves required. 100% of captured revenue is immediately liquid and available for treasury deployment.

Curing the Micro-Deposit and FX Tax

We previously explored how a standard $0.30 gateway flat fee instantly cannibalizes 6% of a casual $5 player deposit. A typical card payment takes a percentage plus this fixed component, and that's before factoring in processor markups, 3-D Secure compliance costs in Europe, or foreign exchange (FX) spreads.

Stablecoins directly fix this "card-rail tax". By routing eligible transactions through stablecoin rails, processing costs are cut to fractions of a percent, directly improving unit economics. Over millions of micro-transactions, this recovered margin is transformative. It allows operators to confidently price in true micro-increments, run regional pricing without FX anxiety, and fund healthier reward loops, like loyalty perks or creator bonuses, without punishing their average revenue per user.

Programmability: Logic at the Money Layer

Stablecoins are not just a cheaper checkout option; they function like an economic operating system. By utilizing smart contracts, operators can establish self-running economic rules directly at the money layer.

Smart contracts automate revenue splits, payouts, rebates, and refunds triggered instantly by on-chain events, such as a match result or quest completion. Because the unit of account is stable, these incentives remain durable and predictable, anchoring rewards to a known value without overnight fluctuations. This programmability removes the manual remediation labor that plagues traditional operations, resulting in fewer drop-offs and a much more reliable player experience.

Treasury Transformation: From Idle Cash to Active Assets

Holding core operating cash in volatile tokens can turn a good season into a balance-sheet problem, proving that treasury management and speculation do not mix. However, treating fiat-pegged stablecoins as a dedicated treasury sleeve allows operators to preserve purchasing power and simplify cross-border flows.

Instead of leaving capital idle in rolling banking reserves, operators can utilize tokenized cash equivalents and permissioned money-market products to generate conservative, single-digit annualized returns (around 3% to 6%). This turns liquidity management from a cost center into an asset, capable of funding live-ops needs, seasonal events, or creator grants. Furthermore, for studios operating in highly inflationary markets holding reserves in USD-pegged stablecoins like USDC or USDT protects their earnings from local currency devaluation and offers fast, low-fee global liquidity.

Bankroll-as-a-Service: Verifiable Liquidity and Trust

While stablecoins optimize how capital moves, Web3-native platforms like DeGaming are utilizing this infrastructure to rethink how capital is verified and deployed. A defining feature of this shift is the introduction of "Bankroll-as-a-Service," powered by proprietary technologies like DeGaming's Glass Vault.

Traditionally, players have been asked to blindly trust that an operator has sufficient liquidity to cover their winnings. By bringing core operations on-chain, Glass Vault provides real-time "proof of funds," offering independently verifiable visibility of platform balances, transactions, and automated payouts.

Because all transactions run through an on-chain engine, operators gain access to scalable liquidity without heavy capital constraints, directly supporting growth and platform stability. Simultaneously, players are given real-time visibility into the exact funds available on the platform they are playing on. This model eliminates the traditional "casino black box," making trust verifiable by design and removing a significant barrier to scaling for operators.

Can a Federal Reserve decision break your iGaming platform?
written by Álvaro Herráez González on chain intelligence analyst.

The reality of today's GambleFi sector is clear: retail liquidity has permanently contracted, and global pools are operating in highly constrained environments. The financial cushion is gone, meaning platforms no longer have the luxury of deep margins to absorb unexpected macroeconomic liquidity crunches or sudden withdrawal spikes. When central bank tightening dries up market liquidity, user withdrawal requests spike unpredictably. If a platform’s corporate treasury is left floating entirely on congested cross-chain bridges or secondary L2 execution layers, the operator will face aggressive slippage and critical payment delays, which instantly destroys player trust in the iGaming industry.

The solution lies in implementing automated, programmatic sweeping pipelines that dynamically redirect net operational revenues from high-frequency layers into institutional-grade settlement vaults on Ethereum or TRON, where over 80% of global stablecoin liquidity securely resides. Operators must protect their solvency buffers before the next macro contraction hits.

For a granular breakdown of the automated sweeping pipelines, algorithmic risk triggers, and the four-tier metric matrix required by corporate treasury to measure network friction, access our deep-dive framework at https://blockchaingamealliance.net/cfo-igaming/].

3.3 TRANSPARENT AND COST-EFFECTIVE COMPLIANCE

The historical paradigm of regulatory compliance in iGaming is undergoing a systemic shift. Globally, licensing bodies are no longer accepting manual, retroactive reporting where compliance teams scramble to compile disjointed spreadsheets on the eve of an audit. The regulatory perimeter has tightened; the new baseline demands proactive, verifiable data trails.

The scale of this enforcement era is clear:

- **The Velocity of Enforcement**: In its latest data, the UK Gambling Commission (UKGC) revealed it executed over 9,700 compliance actions, more than doubling the 4,200 actions from the previous period.

- **The Systemic Collapse:** This administrative surge has exposed severe structural vulnerabilities in legacy setups, with one in four operators failing to achieve satisfactory compliance ratings.

- **The "Reconstruction" Crackdown**: Regulators are explicitly penalizing platforms that must reconstruct manual transaction logs and player histories after the fact.

- **The Looming EU Single Rulebook**: While the European Union's landmark Anti-Money Laundering Regulation (EU 2024/1624) officially takes effect in July 2027, the operational runway is being built right now across 27 fragmented national jurisdictions, forcing operators to deploy real-time risk assessments and immutable transaction architectures today.

Faced with an unsustainable administrative burden, the industry must transition to a technological framework where data integrity is automated at the core.

REGULATORS ····· AUDITORS ····· COURTS

REAL-TIME TELEMETRY

- Continuous audit trails
- Read-only regulator access
- Proof of funds

SYSTEM-ENFORCED INTEGRITY

- Hardcoded risk controls
- Automated payouts
- No post-event tampering

COURT-ADMISSIBLE FORENSICS

- Deterministic attribution
- Fewer false positives
- Evidence provenance

IMMUTABLE LEDGER + PERMISSIONED DATA LAYER

The shared infrastructure that records activity, enforces rules, and preserves evidentiary trails in real time.

REAL–TIME TELEMETRY

- Continuous audit trails
- Read-only regulator access
- Proof of funds

Pillar 1: Transitioning from Retrospective Audits to Real-Time Telemetry

The legacy operational stack forces compliance teams to spend hundreds of manual hours pulling database logs and reconciling batch-processed banking files. This architecture is highly vulnerable to human error and data distortion. By utilizing an on-chain verification infrastructure (such as DeGaming's proprietary Glass Vault ledger) operators transition from reactive reporting to live telemetry:

- **Continuous Audit Trails**: Every wager, deposit, and automated settlement is written to a permissioned ledger in real time, creating an unalterable proof of activity.

- **Eliminating the Reporting Tax**: Instead of compiling lagging documentation for audits, operators can grant regulators permissioned access to a real-time, read-only validator viewport. This allows authorities to verify Gross Gaming Revenue (GGR) and tax liabilities on-demand, completely eradicating the administrative friction of manual submissions.

- **Verifiable Balance Liquidity**: The ledger provides real-time "proof of funds," satisfying strict financial stability mandates without exposing sensitive, off-chain corporate structures.

ULLE SKOTTLING
CEO OF DEGAMING

"The purpose of the blockchain is not to keep things anonymous... it's the purpose to keep check on things."

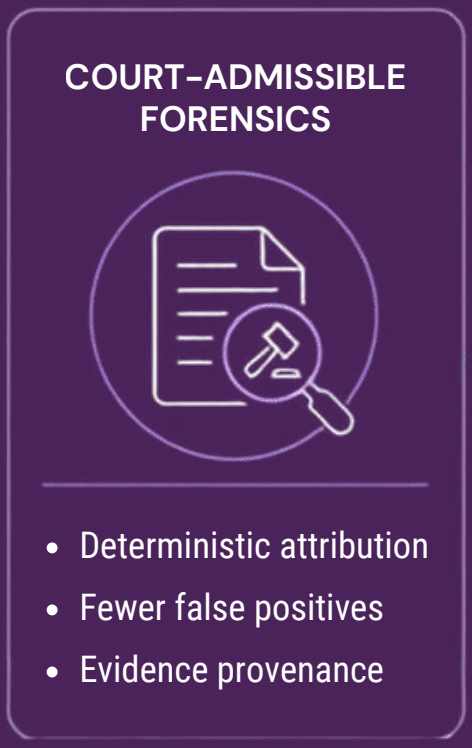
Pillar 2: System-Enforced Operational Integrity

Compliance failures frequently trace back to post-event back-office manipulation or flawed manual interventions. To survive a climate where 25% of operators are failing basic assessments, compliance-by-design must be hardcoded into the platform application layer.

- When platform rules are structurally enforced by the underlying engine, systemic non-compliance is mathematically prevented:

- Algorithmic Risk Controls: Betting thresholds, maximum exposures, and player safety limits are hardcoded. Back-office staff cannot manually manipulate historical ledgers, distort RTP margins, or retroactively alter player activity.

- Eradicating Payout Disputes: Smart contract logic handles the custody and distribution of wagers based on verified game outcomes. Payouts trigger instantly to non-custodial wallets, removing human bias and eliminating the customer disputes that trigger costly regulatory reviews.



Pillar 3: Court-Admissible Forensics & Standardized Analytics Ontologies

While clean ledger infrastructure stops internal system tampering, managing external financial crime risk requires a standardized framework to interpret on-chain data flows. Operators cannot rely on opaque, "black-box" risk scores that trigger false positives, drive customer churn, or fail to withstand regulatory cross-examination.

To bridge the gap between underlying data availability and high-stakes anti-money laundering (AML) compliance, the industry must adopt formalized analytical frameworks, such as the Address Clustering Ontology pioneered by Chainalysis.

By applying a structured ontology to blockchain analytics, operators transition from probabilistic guesswork to highly defensible compliance records:

- Deterministic Entity Attribution: Rather than guessing wallet ownership using unverified machine learning loops, the platform relies on formalized clustering methodologies. This separates structural interaction data from speculative inferences, ensuring that user wallets are only linked to entities based on documented, verifiable heuristics.

- Mitigating Attribution Errors: By cleanly mapping out blockchain edge cases, such as explicitly isolating nested exchange infrastructure or identifying and stripping out CoinJoin mixing layouts, the compliance engine significantly reduces false positives. This protects player lifetime value (LTV) by preventing wrongful account terminations while ensuring legitimate sanctions risks are accurately flagged.

- **Evidentiary Data Provenance**: Compliance tracking moves beyond passive data collection. In alignment with strict judicial and auditing standards (such as the Daubert standard used in federal court reviews), every transaction alert is backed by an audit trail of empirical evidence—ranging from law-enforcement-verified ground-truth datasets to verified undercover transaction paths.

Ultimately, this forensic architecture ensures that the operator's AML compliance data is no longer a localized, debatable claim, but an immutable, standardized record capable of withstanding the most aggressive regulatory audits on earth.

3.4 IDENTITY AGAINST MODERN FRAUD

*Produced in collaboration with **JustALab** | **All sources available on Apendix 2***

The Problem Traditional KYC Can No Longer Solve

The iGaming industry's fraud problem has quietly evolved into a structural challenge that traditional compliance stacks were never built to handle. Traditional KYC was designed under the assumption that a real person matches the physical documents they submit. While this assumption held when fraud was limited to stolen credit cards or borrowed identities, it has completely broken down against modern synthetic threats.

- 78% of North American operators now cite this trend as their top operational threat.
- The current compliance layer generates mounting transactional costs without providing actual security, creating an environment where operator verification budgets grow annually while attacks consistently outpace defenses.
- Ultimately, traditional KYC adds heavy friction for legitimate players while failing to stop sophisticated fraudsters.

What Decentralized Identity Actually Solves

Decentralized identity (DeID) does not replace fraud detection; instead, it changes the underlying architecture that fraud currently exploits.

The multi-accounting problem has a structural cause: platform identity is cheap to duplicate. An email address costs nothing. A phone number costs a dollar. A KYC document, increasingly, costs twenty. As long as identity is something a player is asked to produce, it can be produced at scale by anyone motivated to do so.

Decentralized identity introduces a two-layer structural fix working in tandem, supported by portable reputation networks and cryptographic privacy tools:

1. Passkey Authentication
Modern passkeys generate a private key inside the hardware secure enclave of a device, the same chip that powers Face ID and fingerprint unlock. That key never leaves the device. It cannot be copied, exported, or synthesized, and it cannot be phished. When a player's account is secured by a passkey, the root of trust shifts from a document or password (both of which can be fabricated or stolen) to hardware-bound cryptography.

2. The Credential Layer

While passkeys verify device legitimacy, verifiable credentials establish the legitimacy of the person operating it. A KYC provider or other trusted issuer attaches a signed

attestation to the player’s onchain identity : age confirmed, identity verified, jurisdiction cleared. Any operator can verify that credential without repeating the check. One human, one credentialed identity, enforced by the issuer. The cost of running a multi-account operation stops scaling with email addresses and starts scaling with the ability to produce genuinely new, verified humans.

3. Portable Identities and ENS Subnames

Ethereum Name Service (ENS) subnames provide players with a persistent, portable on-chain identity (e.g., alex.casino.id) that travels seamlessly across different platforms. Instead of forcing every platform to rebuild a player's risk profile from scratch, the subname accumulates a verifiable history over time to establish a portable reputation.

An account with two years of onchain activity, linked social verifications, and an established transaction history presents a fundamentally different risk profile than one created yesterday.

This history becomes a portable reputation ; one the player owns and carries, rather than one each platform rebuilds from scratch.

4. Cryptographic Privacy via Zero-Knowledge Proofs

The natural concern with onchain identity is public visibility. A player whose gambling activity is readable on a public ledger faces real risks: exposure to targeted scams, personal security threats for high-value players, and unwanted disclosure of behavior they have every right to keep private. Zero-knowledge proofs resolve this directly. A player can prove a specific claim to an operator that they are over 18, that they have passed KYC, that their account has two or more years of verified history ; without exposing the underlying data to anyone. The verification exists. The proof is auditable. The details are not public. Operators get the compliance signal they need. The player's history remains their own.

Concrete Use Cases in iGaming

The deployment of decentralized identity in iGaming is not a single use case. It is a structural layer that changes the economics of fraud, the portability of compliance, and the privacy model of player verification. The table below maps the main operator pain points to the specific DeID mechanisms that address them.

iGaming problem	*Why current KYC fails*	*DeID mechanism*	*Business impact*
Multi-accounting & bonus abuse	Email addresses, phone numbers, and synthetic documents are cheap to reproduce at scale.	One verified credential tied to a passkey-secured identity.	The economics of bonus abuse break because attackers need real, verified humans instead of disposable accounts.
Synthetic identity fraud	Document upload creates an attack surface for AI-generated faces, forged IDs, and fake liveness checks.	Registration relies on passkeys and reusable credentials instead of repeated document submission.	The deepfake-document surface is reduced because the operator verifies a credential, not a newly uploaded document.
Cross-platform fraud rings	Operators verify players independently, with little shared signal across platforms.	Portable ENS-linked identity and reusable reputation signals.	Risk scoring improves because operators can distinguish established identities from fresh, disposable accounts.

iGaming problem	*Why current KYC fails*	*DeID mechanism*	*Business impact*
Repeated KYC cost	Every operator repeats the same document, liveness, and manual review workflow.	A trusted issuer verifies once and issues a reusable verifiable credential.	Compliance friction and duplicated verification cost fall across the ecosystem.
Player privacy & data exposure	Raw documents and activity histories create liability and exposure risk.	Zero-knowledge proofs verify claims without exposing underlying personal data.	Operators receive compliance signals while holding less sensitive player data.
Onboarding drop-off	More verification steps mean more abandoned registrations.	Passkey login, invisible ENS issuance, and credential checks in the background.	Legitimate players onboard faster, while fraud resistance improves.

The Business Case: One Identity, Multiple Brand Profiles

dd

The UX Argument: Less Friction, Not More

The legitimate concern from operators is always the same: anything that adds steps to onboarding loses players. The decentralized identity (DeID) model addresses this directly.

With JustaName's infrastructure, ENS subname issuance is gasless and invisible to the player. They register with a biometric passkey, the same Face ID gesture they use to unlock their phone. Their name.casino.id identity is issued automatically in the background. No public address. No seed phrase. No understanding of blockchain required.

From the player's perspective, it is a faster and smoother onboarding than current KYC flows : no document upload, no waiting for manual review, no re-verification when they return after six months. Their identity is theirs, stored on their device, ready to use. And their history, however long, however active ; is never a public record unless they choose to make it one.

This is the experience that platforms integrating JAW.id : a smart account SDK that pairs passkey authentication with ENS identity issuance, can offer their players out of the box without building any of this infrastructure themselves; all in 2 lines of code.
The compliance gain is real. The friction cost is near zero.

Conclusion

For operators ready to move beyond the document-verification model, decentralized identity is not a replacement for compliance ; it is an upgrade to the foundation compliance runs on. Infrastructure like JAW.id makes this upgrade deployable today: passkey-secured smart accounts paired with ENS identity issuance, available through a single SDK integration, without rebuilding existing onboarding flows. An upgrade the next generation of synthetic fraud cannot bypass with a JPEG.

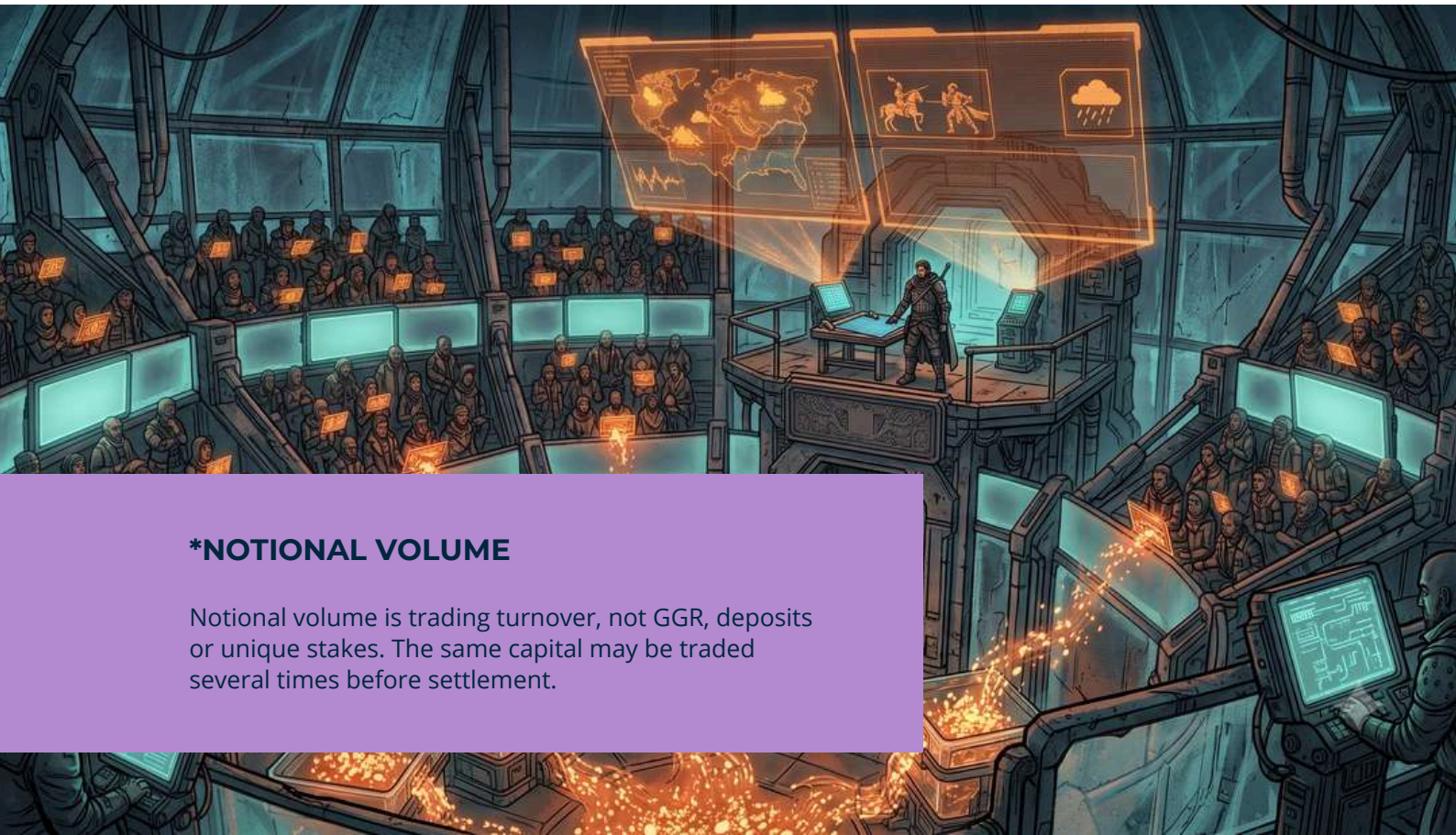
ACT IV THE PREDICTION MARKET A NEW HORIZON OF GROWTH

Across regulated exchanges and on-chain platforms, prediction markets have moved far beyond their political-season origins. By combining exchange-style pricing with real-time markets around sports, politics and global events, they have become one of the fastest-growing products adjacent to sports betting.

After processing $75.7 billion in notional volume in Q1 2026, the category reached a record $113.8 billion in Q2 (an increase of 48.7% quarter-on-quarter). June alone generated $52.8 billion, almost twice January's previous monthly record. Notional volume is not equivalent to GGR or unique stakes, but the acceleration is now too significant for iGaming operators to ignore.

From Political Novelty to Sports Powerhouse

Prediction markets first captured mainstream attention during the 2024 US election cycle, but sports has become the category's principal growth engine. Sports already represented roughly 80% of Kalshi's Q1 volume. By June, it had also risen from 40% to 81% of Polymarket's activity, demonstrating that the shift is now category-wide rather than platform-specific.

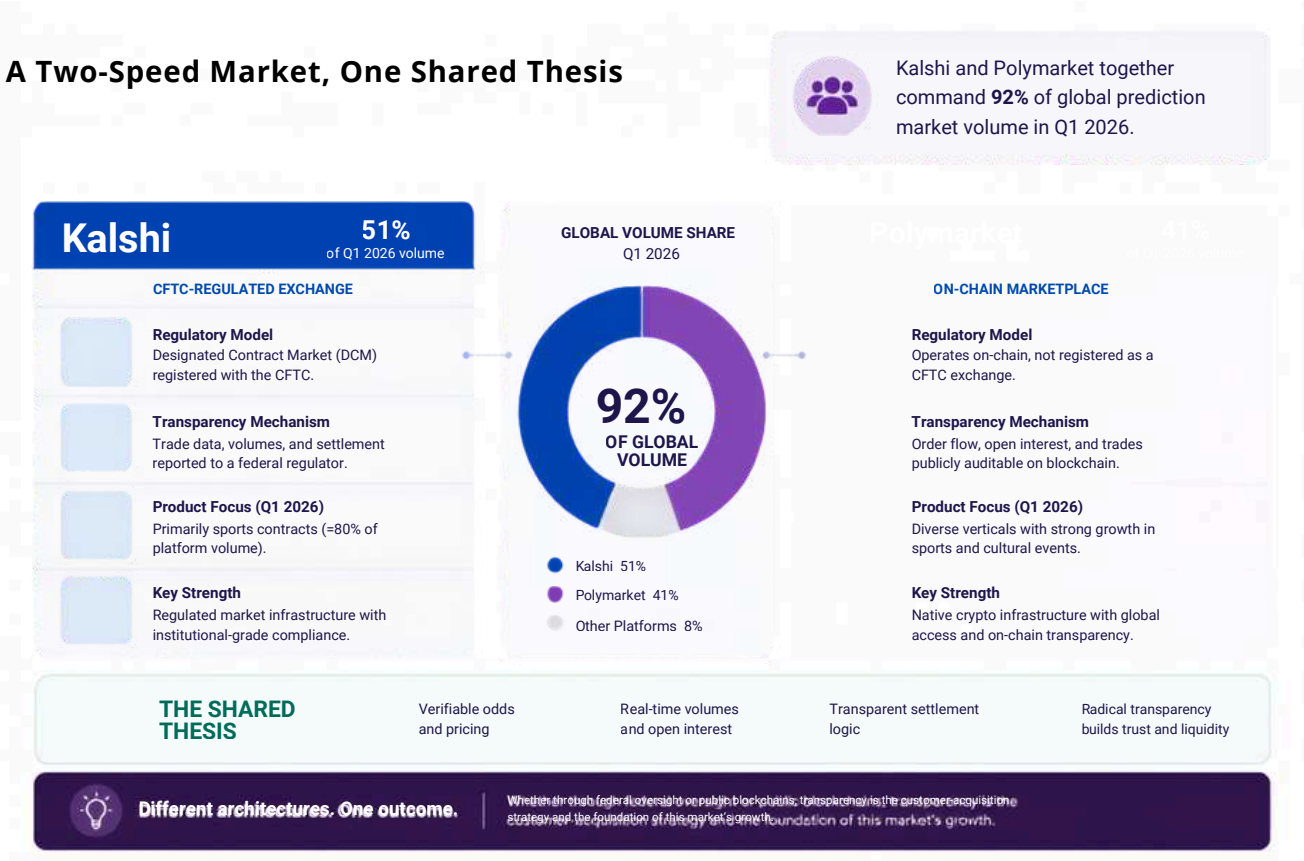


***NOTIONAL VOLUME**

Notional volume is trading turnover, not GGR, deposits or unique stakes. The same capital may be traded several times before settlement.

perfect-bracket jackpot, and the NBA playoffs) drove successive monthly records. Politics, by comparison, accounted for $7.9 billion across all platforms in the quarter. The strategic implication for iGaming is direct: prediction markets are no longer courting a separate audience. They are converging on the sportsbook's core product, repackaged as a trading interface rather than a betslip, and expanding into casual verticals (culture, entertainment, weather, and combo/parlay-style products) that mirror exactly the casualization trend.

A Two-Speed Market, One Shared Thesis



The Capital Stampede

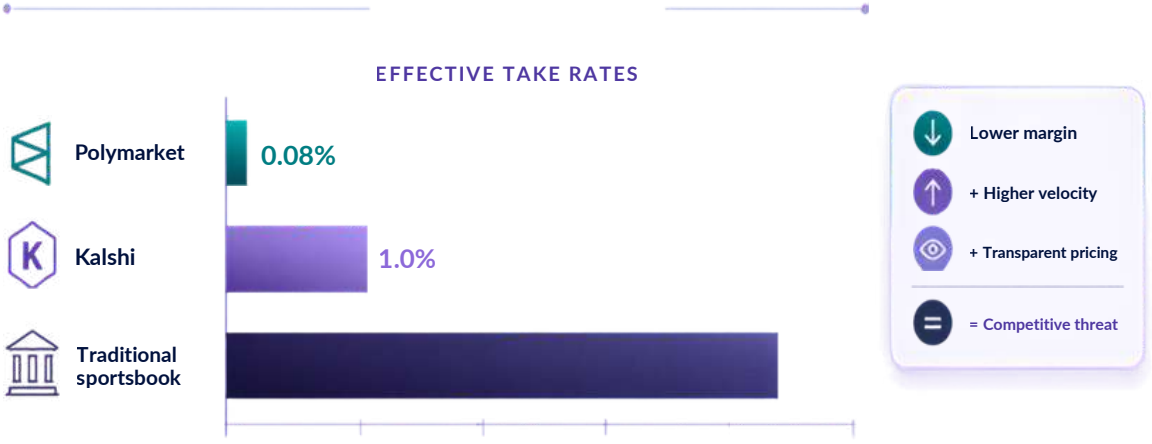
Institutional capital validated the category at unprecedented speed in early 2026. Sixteen venture rounds raised $1.725 billion in a single quarter, the largest amount in the category's history, led by Kalshi's $1 billion Series F at a $22 billion valuation and an additional $600M investment in Polymarket by Intercontinental Exchange, the parent company of the New York Stock Exchange.

Eight M&A deals closed over the same period, several of them explicitly regulatory plays: Robinhood and Susquehanna formed the Rothera joint venture, which acquired MIAXdx., while Underdog bought Aristotle Exchange to own a registered exchange rather than rent one. The incumbents are no longer observing. Robinhood traded over 12 billion event contracts in 2025 and calls prediction markets the fastest-growing product in its history; DraftKings has integrated prediction markets into its unified Sports app, extending its reach nationwide, although market availability varies by jurisdiction.; Fanatics launched a standalone prediction app across 24 states; and Goldman Sachs, JPMorgan and Interactive Brokers are each exploring CFTC-regulated prediction infrastructure.

Source : State of Prediction Markets 2026 / State of Prediction Markets Q2 2026

The Margin Question, and a Familiar Threat

The counterweight to this euphoria is monetization. Effective take rates run from 0.08% at Polymarket, which only switched on its first trading fees in January 2026, to roughly 1.0% at Kalshi, which converted an estimated $33.1 billion of volume into approximately $331 million of quarterly revenue. Compared with the mid-to-high single-digit hold of a traditional sportsbook, the strategic threat becomes clear: prediction markets are a structurally cheaper way to take a position on a sporting event. The industry has seen this movie before. Act I described how offshore rails siphoned liquidity from licensed operators by simply being cheaper, faster and more frictionless. Prediction markets repeat that pattern from inside the regulated perimeter, holding a CFTC registration instead of a Curaçao licence. The lesson for operators is not to take comfort in the thin margins, but to recognise that razor-thin, high-velocity, fully transparent pricing is precisely what the next generation of bettors is choosing.



Integrity Is the Price of Admission

Prediction markets promise radical transparency, but a visible market is not automatically an honest one. An on-chain record can prove that a trade occurred and show how a contract settled. It cannot, by itself, establish that the activity was organic, that apparently independent wallets were controlled by different people, or that traders had no ability to influence the result.

That distinction becomes more important as the category scales. A 2025 working paper by Columbia researchers identified transaction patterns consistent with wash trading across roughly a quarter of Polymarket's historical volume. Artificial volume does more than exaggerate activity: it can distort perceptions of liquidity, attract copycat traders and make a market price appear more informative than it really is. Research also suggests that well-capitalised participants can temporarily move implied probabilities, particularly in thinner markets where users interpret price movement itself as new information.

The 3 attach surfaces :
1 - PRICE
Coordinated trading, wash trading or concentrated positions can distort liquidity and the probability displayed to the public.

2 - EVENT
Insiders or participants may trade on non-public information, or take positions on outcomes they are capable of influencing.

3 - RESOLUTION
A trader may attempt to compromise the oracle, data source or underlying measurement used to determine the winning contract.

The public ledger is nevertheless an advantage. Activity that could disappear inside closed databases becomes available for continuous surveillance and retrospective investigation. But pseudonymous transparency has limits. Detecting a suspicious wallet is not the same as identifying the person behind it, linking related accounts or proving a conflict of interest.

For prediction markets to enter regulated iGaming, integrity must therefore be designed across both the trading and resolution layers. That means accountable identity, multi-account detection, conflict-of-interest controls, position limits and circuit breakers, real-time monitoring for coordinated activity, transparent market rules, and multi-source resolution mechanisms supported by a documented dispute process. Verifiable credentials and tamper-evident telemetry can enable those controls without placing every piece of personal information on a public chain.

Prediction markets do not need less oversight because their order books are visible. They need oversight capable of using that visibility. The blockchain opportunity is not merely to place event contracts on-chain, but to produce evidence that operators, auditors and regulators can interrogate before, during and after the market.

The Regulatory Stress test : When the market can change the event

Market integrity asks whether the price can be trusted. Prediction markets force regulators to confront a second, more fundamental question: should every event be tradable at all?

Unlike a casino spin, many of the events underlying these contracts are not sealed off from the people trading them. A participant may possess non-public information, be able to influence the outcome, or control the source used for resolution. Once a financial position is attached to an election, corporate announcement, weather reading, sporting action or geopolitical event, the market can create incentives that extend beyond the wager itself.

France's ANJ has warned that when traders can affect an outcome, event contracts may create incentives to sabotage a sporting performance or provoke harmful geopolitical actions. The Dutch KSA has similarly raised concerns about the potential influence of election markets. These are public-interest externalities: the market no longer simply observes reality; it risks becoming part of the causal chain producing it.

This should not be confused with evidence that prediction markets routinely destabilise democracies. More liquid markets may correct deliberate price distortions, and their forecasting value is real.

But the regulatory test is not only how frequently manipulation succeeds. It is whether a product creates a credible incentive for officials, insiders, athletes or technical operators to profit from decisions and systems they control.

What opportunity remains for iGaming ?

For iGaming, this is not the end of the opportunity but its definition. Operators can launch event contracts where both the product category and distribution model are explicitly permitted; incorporate exchange-style pricing and transparent liquidity into existing licensed betting products; or supply the underlying B2B infrastructure for identity, surveillance, escrow and resolution.

The advantage of regulated operators is not their ability to move faster than offshore platforms. It is their experience with player protection, geolocation, responsible gambling, sports integrity and accountable distribution. Combined with the verification stack described in Act III, those capabilities can transform prediction-market mechanics into a controlled and defensible product.

Prediction markets are therefore both a proof of demand and a regulatory stress test. Blockchain can make a market more observable, auditable and accountable; it cannot determine which events society should allow people to trade. Prediction markets may become iGaming's next chapter, but only where market integrity, consumer protection and jurisdictional permission advance together.

UPDATE SEPT 2026 : CLARITY ACT REJECTED

While the Senate's rejection of the CLARITY Act on September 15, 2026, delivered a sharp, unexpected setback to establishing a unified federal preemption framework for prediction markets, it has also catalyzed a vital phase of industry maturation. Platforms like Kalshi are currently navigating localized legal friction with state regulators in jurisdictions like Nevada, Iowa, and Utah. However, much like the early state-by-state rollout that ultimately built the multi-billion-dollar U.S. sports betting market, this pushback is forcing essential dialogue. Rather than stalling the sector, these state-level challenges are driving rapid innovation in state-federal compliance technologies, localized licensing models, and bulletproof market integrity standards, paving a far more resilient, battle-tested path for prediction markets to scale safely across the U.S.

ABOUT THE CONTRIBUTORS

DeGaming

DeGaming is a business-to-business Web3 crypto iGaming infrastructure provider that enables operators to launch fully transparent, white-label online casinos in just fourteen days. By leveraging blockchain technology, the company replaces the opaque nature of legacy gambling platforms with a verifiable ecosystem where every bet, payout, and balance is executed on-chain and remains independently auditable.

The Glass Vault Architecture

At the heart of the platform is the Glass Vault, which serves as an on-chain verification layer designed to build unbreakable player trust. This system ensures that every financial movement is permanently recorded on the blockchain, meaning bets and payouts are executed according to fixed system rules. This prevents manual manipulation of outcomes, eliminates settlement disputes, and secures operations through cryptographic proof rather than operator promises.
Turnkey White-Label Ecosystem

Operators receive a fully managed platform featuring a customizable frontend, a unified back office, built-in marketing tools, customer relationship management, and automated player retention systems. This comprehensive integration gives businesses instant access to over six thousand casino games without the need to hire developers, manage hosting, or juggle multiple fragmented software vendors.

Bankroll-as-a-Service

Operating an online casino typically requires massive upfront capital to hold large reserves for player winnings, but DeGaming eliminates this barrier. The platform provides external, investor-backed liquidity to cover payout variance and player withdrawals instantly on the blockchain. Because the infrastructure takes on the financial payout risk, operators can direct their capital entirely toward brand growth and player acquisition.

Global Compliance and Market Access

The infrastructure is built to support seamless crypto deposits and instant withdrawals while natively enforcing strict anti-money laundering and know-your-customer protocols. Through automated system whitelisting, operators can confidently launch operations across one hundred and eighty-six countries, bypassing traditional banking delays to scale globally with verifiable security.

ABOUT THE CONTRIBUTORS

This report was produced through the collaboration of :

Gaming Malta

Gaming Malta is a government-backed foundation that promotes Malta as a global hub for video games, esports, and digital entertainment, supporting studios with ecosystem development, talent initiatives, and international visibility. It acts as a strategic bridge between industry and government to attract investment and grow Malta's gaming sector.

Malta Gaming Authority (MGA)

MGA is Malta's national gambling regulator responsible for licensing, supervising, and enforcing rules for online and land-based gaming operators. It ensures player protection, fair play, and compliance, making Malta one of the world's most reputable jurisdictions for iGaming regulation.

JustAName

JustaName is an identity-first Web3 infrastructure provider that enables brands to issue portable, human-readable ENS-based digital identities directly within their products. The platform focuses on frictionless onboarding, brand-powered naming, and interoperable identity layers that work across Ethereum, L2s, and even non-EVM networks.

Álvaro Herráez González

On-chain intelligence analyst specialized in blockchain forensics, fraud investigation, and financial crime analysis. With a background in fraud detection and data analytics within large-scale financial systems , Alvaro focuses on tracing illicit flows, identifying laundering patterns, and analyzing behavioral dynamics of on-chain actors.

APPENDIX

Annexe 1

Global iGaming Market Sizing Estimates for 2025 and Projected Growth

Research Organization	2025 Sizing (USD)	Projected Sizing (USD)	Projected Year	CAGR & Forecast Period
Voluum Research	$117.50 Billion	$186.58 Billion	2029	12.30% (2025–2029)
iGaming Today Consensus	$107.00 – $118.00 Billion	N/A	N/A	8.00% – 11.00% Year-over-Year
Custom Market Insights (CMI)	$88.44 Billion	$245.45 Billion	2034	12.01% (2025–2034)
Grand View Research	$88.00 Billion	$202.80 Billion	2033	11.00% (2026–2033)
Straits Research	$85.31 Billion	$220.01 Billion	2034	11.10% (2026–2034)

APPENDIX

Appendix 2
Sources

1. Zyphe : "How Fraudsters Are Beating Your KYC With $20 Deepfakes" https://www.zyphe.com/resources/blog/how-fraudsters-are-beating-your-kyc-with-20-deepfakes
2. KYC-Chain : "AI Identity Fraud & Deepfakes: Liveness Defenses in 2025" (244% document forgery growth) https://kyc-chain.com/ai-identity-fraud-2025/
3. Veriff : "iGaming Fraud Prevention: How Platforms Stop Bonus Abuse and Multi-Accounting" (automated scripts, under one minute per account) https://www.veriff.com/fraud/learn/igamingfraud
4. PRNewswire : "Bonus Abuse Emerges as the Most Widespread Form of Online Gaming Fraud in North America" (78% of operators, $1B lost in 2024, 64% rise) https://www.prnewswire.com/news-releases/bonus-abuse-emerges-as-the-most-widespread-form-of-online-gaming-fraud-in-north-america-302705393.html
5. Shuftipro : "iGaming Fraud Prevention: Bonus Abuse and Multi-Accounting" (50%+ of all iGaming fraud cases) https://shuftipro.com/blog/igaming-fraud-prevention/
6. FATF Horizon Scan, December 2025 : Deepfakes identified as capable of bypassing AML controls and digital ID verification at onboarding https://www.fatf-gafi.org
7. Apple Platform Security : Secure Enclave (passkey private key generation and hardware binding) https://support.apple.com/guide/security/secure-enclave-sec59b0b31ff/web
8. Ethereum Name Service Documentation : ENS Resolution and Name Records https://docs.ens.domains
9. W3C : "Verifiable Credentials Data Model 2.0" (foundational specification for cryptographically signed identity attestations)
10. https://www.w3.org/TR/vc-data-model-2.0/
11. Ethereum Foundation : "Zero-Knowledge Proofs" (technical overview of ZK proof mechanisms) https://ethereum.org/en/zero-knowledge-proofs/


BGA
BLOCKCHAIN
GAME
ALLIANCE