LUISS

Degree Program in Economics and Business (Major in Management)

Course of Blockchain and Cryptocurrencies

Provably Fair Systems in Crypto Gambling

Prof. Massimo Bernaschi

SUPERVISOR

Edoardo Soppa 283611

CANDIDATE

Academic Year 2024/2025

Table of Contents:

Introduction:

Context and motivation:

Online gambling has experienced exponential growth over the last decade, driven by both the digitalization of gambling platforms and the increasing popularity of crypto casinos.

However, this rise has not been accompanied by an increase in user trust; traditional platforms operate as black boxes, where users are expected to accept outcomes without any insight on how these results are generated, in an industry where financial incentives are the highest and regulation is fragmented skepticism regarding actual fairness is inevitable.

Blockchain technology, merged with cryptographic techniques, offers a paradigm shift.

Provably fair systems seek to address these concerns by enabling users to verify the integrity of each game round as an independent event; these systems provide transparency by offering mathematical proof, yet this concept remains largely misunderstood by the average user.

This thesis investigates whether these systems live up to their promise, and, if not, what still stands in the way.

Scope of the thesis:

This research focuses on the concept of provably fair gambling within crypto-based casinos.

It will explore the mechanisms, their implementation (e.g. On Stake.com), and the role of blockchain in enabling trustless environments.

Social dimension is also considered to determine whether users actually verify results or, “provably fair” is just another marketing buzzword.

This thesis does not cover broader regulatory/psychological aspects of gambling, instead it concentrates on the technological and perceptual aspects of transparency and fairness, as they relate to cryptographic methods.

Methodology:

This research is primarily qualitative and analytical, drawing on documentation from existing platforms, white papers and reputable secondary sources, such as industry reports and academic articles.

Chapter 1: Provably Fair Systems in Crypto Gambling

1.1) The Rise of Online Gambling and the Trust Problem

Online gambling has grown exponentially, especially after 2010s, this is due to increasing internet penetration, mobile-first gaming interfaces, different law regulations (e.g. in Italy there are a limited number of casinos), crypto integration enabling borderless transactions.

This expansion led to the rise of crypto casinos, which operate 24/7, globally with minimal KYC (Know Your Customer).

The core problem of traditional online gambling platforms is the lack of trust, as they rely on centralized systems, random number generators and hosted server-side, therefore players have no direct access to the logic/code determining the outcomes, this leads to a "black box model", which often leads to distrust on the RTP (Return to Player).

Even in jurisdictions which provide clear and fair licensing operations vary in how strict monitoring occurs; certification by third-party labs (like eCOGRA) exists however it is still not transparent to players and requires trust in the certifier.

Today, players are more informed, particularly in the crypto-native community, this translates into increasing demand for game logic transparency, fairness assurance, and autonomous verification of outcomes.

Provably fair systems emerged in Bitcoin-based games, such as dice (player chooses a threshold number between 0 and 100, if the outcome falls below the threshold, player wins a multiplier-based payout), and crash (a multiplier line begins at 1.00x and rises exponentially, players place a bet before the round begins and must "cash out" before the line crashes, if they don't, they lose the bet).

These systems were designed to remove the need for blind trust, with users able to verify every game result independently.

With gambling being a high risk, high reward environment trust is everything, without a credible way to verify fairness platforms lose reputational capital, therefore both new user acquisition and retention suffer.

Provably fair systems are not just a tech feature; they are a credibility framework.

1.2) The concept of "Provably Fair"

As we previously stated, provably fair is a system that allows players to independently verify the fairness of each game's outcome, it emerged from early Bitcoin gambling sites like Primedice and Bustabit (which originally had no ID verification requirement), where community's skepticism was high and user transparency was key.

Unlike traditional casinos, PF (Provably Fair) doesn't rely on trust in the operator, but on mathematical evidence.

In simpler terms, traditional online gambling says: "trust us, it's fair", while provably fair gambling says: "here's the math, prove it yourself".

PF introduces verifiability, transparency and, potentially, decentralization into game outcomes.

SoftSwiss (through BGaming) is a leader in implementing provably fair technology in commercial crypto gambling: their systems allow players to customize or input their client seed, verify their server seed hash before gameplay, get access to server seed and nonce post-game, and use built in external tools to recompute and confirm the game result.

Key cryptographic components are:

1) **Server Seed**
   - Generated by the casino.
   - Hidden from the player until the end of the session.
   - Pre-hashed and shown before the round starts to commit to the outcome.
2) **Client Seed**
   - Chosen by the player or randomly generated.
   - Allows partial control of randomness (adds transparency).
3) **Nonce**
   - A counter that increases with every bet.
   - Ensures each round is unique.
4) **Hash Function (e.g., SHA-256)**
   - Combines server seed, client seed, and nonce to create a deterministic outcome.
   - Makes it computationally infeasible to fake results.
5) **Post-Game Verification**
   - After the round, server seed is revealed.
   - The player can use SHA-256 or tools to verify that the outcome matches the committed hash.

This works because the PF model is based on a commit-reveal scheme, first the casino commits to a value by hashing the server seed and sharing the hash, then the player adds input (client seed), and the game executes, the casino then reveals the server seed, so that everyone can recompute and verify its outcome.

This procedure is similar to Pedersen Commitments (a cryptographic technique used to "lock in" a value without revealing it), both PF and PC (Pedersen Commitments) use binding (cannot change the value after committing) and hiding (don't reveal the value before you choose to).

Both use cryptographic principles to ensure integrity and privacy until they are revealed.

The main difference between them is that Pedersen uses elliptic curve math, while PF uses simpler hash functions (SHA-256), but the logical structure is the same.

1.3) How Provably Fair Systems Work: A High-Level Overview

Here is a step-by-step breakdown of the Provably Fair Mechanism:

1. Commitment Phase (before the game starts)
    - Casino server generates a random value called server seed
    - A hash of the server seed is created using a secure algorithm like SHA-256
    - Hashed server seed is shared with the player before the game begins, acting as a cryptographic commitment to a fixed, unchangeable value.
2. Player input
    - Player supplies a client seed, which can be generated randomly or customized manually by the player
    - This adds user-side randomness and makes the final outcome less predictable for the operator (similar to cutting the deck in a card game)
3. Nonce Generation
    - A nonce (counter starting from 0 or from 1) increases with every round/bet
    - Its purpose is to ensure that even if the client/server seeds are reused, every outcome is unique.
4. Outcome Calculation
    - The actual game result (e.g. dice roll number or crash multiplier) is computed by combining server seed, client seed and nonce.
    - A cryptographic function (often SHA-256 or HMAC-SHA-256) is applied to this combination, in order to generate a deterministic but unpredictable outcome
5. Post-Game Reveal
    - Once the game is over, the original server seed is revealed, the player now possesses 3/3 (server seed, client seed, nonce), they can recompute the hash and verify that the result wasn't altered.
6. Independent verification
    - Most platforms include built-in tools or links to third party hash calculators

- Users can input the 3 elements and verify if the outcome matches what was committed to pre-game.

This matters because this process removes the need for trust in the casino operator, with the outcome being mathematically provable.

Chapter 2: Challenges and Limitations of Provably Fair Systems

2.1) Technical and Conceptual Limitations

As previously stated, most users do not know how to verify seeds, hashes or nonces.

This occurs because the verification process often requires manual effort or the use of external tools, therefore for the average player PF is “mathematically fair” but not practically accessible.

In practice, PF if “provably fair” only for those who can interpret and use the tools correctly.

Some platforms “e.g. Stake.com” provide internal verification tools, this introduces the requirement of trust in the verification process itself, even if the game logic is technically fair; unless tools are open-source independence is questionable.

Furthermore, some platforms allow full customization of the client seed, while others generate it or reset it automatically, client seeds may be hidden or regenerated silently without the user control, without full visibility or control, players cannot be sure they are influencing the outcome randomness as claimed.

Additionally, in some games PF is inconsistently applied, the base mechanics are covered by PF logic, however bonus rounds, animation triggers or payout logic may still operate opaquely.

Another factor not often disclosed is the variable house edge, in PF casinos games like Dice have a dynamic house edge based on risk, safer bets (e.g. Roll under 95) may have lower house edges (even less than 1%), while riskier bets (e.g. Roll under 2) may have a house edge > 5%.

This nuance is rarely explained to users. Many assume ‘fairness’ implies flat odds, whereas in traditional casinos the house edge is usually fixed for a given game (e.g., 2.7% in European Roulette) and any variations (like side bets in Blackjack) are often explicitly stated by the croupier.

2.1.1) Implementation Flaws and the Possibility of Cheating Provably Fair Systems

While provably fair systems are cryptographically secure in theory, their real-world robustness depends heavily on how faithfully and transparently they are implemented. For example, improper nonce handling can break uniqueness, if nonces are reused and not incremented properly, results could repeat, this enables replay attacks where users can predict/manipulate outcomes.

Additionally, server seed reuse can make the system vulnerable, if platforms don't rotate server seeds regularly (one session per game) players might detect patterns, which, over time, could lead to the possibility of approximating or brute forcing outcomes.

Another potential weakness is poor random-number generation. If a PF system uses a weak or deterministic source to generate seeds, the results may become predictable despite the hash-based protections.

There's also the possibility of tampering with client-side verification tools. If the 'fairness calculators' or result verifiers are not open source, a malicious platform could manipulate them to display "verified" outcomes even when the results are unfair.

In conclusion, is it possible to cheat PF? Theoretically no (if properly implemented), while practically yes, if, for example, the platform is malicious, seed or nonces are manipulated, client seed customization is restricted or ignored, users blindly rely on closed source verification tools.

It is not about breaking the hash but rather bypassing the integrity of the system's inputs.

2.2) Why Trust is Still Required in Provably Fair Systems

As previously stated, PF could be the next step for trustless gambling, however, today PF ecosystem is not yet fully decentralized.

First, verification tools are not independent, as most platforms have their own verification systems, users still have to rely on the platform's integrity, without open-source code or third-party audits this process lacks true neutrality.

Furthermore, users must trust the honesty of initial values; players can verify outcomes, but not how the server seed was generated in the first place, there is no guarantee that the server seed wasn't preselected to favor the house across multiple rounds, as PF only proves consistency, not that the initial values were fairly chosen.

User control is sometimes limited, in some platforms client seeds are quietly assigned automatically without user interaction (or possibility of reset), this undermines the user input aspect of randomness and could create a misleading sense of fairness.

It is important to specify also that PF systems are technical mechanisms, not legal protection. A game could be provably fair but still violate advertising ethics or regulations, also, the house edge could be even higher than traditional casinos; there is currently no legal standard requiring platforms to implement PF or to prove that it is being used correctly.

In conclusion PF ≠ uncheatable, even if the math checks out, users still have to place trust in the platform's implementation quality, security practices and honesty.

Social trust also matters; players still assess casinos based on brand reputation, endorsements and word of mouth.

2.3) Perception, Adoption and Public Skepticism

Most of the users of PF platforms have no idea what a server seed, client seed and nonce are, platforms rarely offer clear tutorials to explain how PF works, and, even when tools are available, they are hidden or overly technical.

Additionally, players almost never bother to verify game results. The process is often too complex and offers no immediate benefit unless a player already suspects manipulation. In practice, users tend to trust the casino's interface rather than delve into the underlying mechanics.

Some videos on YouTube show large wins being interrupted by suspicious error messages on Stake.com, these clips suggest that Stake may cancel/alter outcomes in real time, the sources are anonymous and unverifiable, they could be authentic, fabricated, or produced by competition.

Regardless of the origin such videos reflect a persistent distrust, even among crypto-savvy users.

PF is often promoted as a feature without real user interaction, some games only implement parts of PF, when users realize this, it creates disappointment and reduces trust in the label itself.

Users are more likely to be influenced by trust in streamers, youtubers and celebrities rather than cryptographic mechanisms; high profile sponsorships (e.g. Drake - Stake.com collab) are used to create a perception of legitimacy, these promotions almost never mention PF, reinforcing the idea that branding > proof.

2.4) Risk of Centralized 'fairness'

Despite the term "provably fair" being associated with crypto casinos, most PF systems are not recorded or verified on a blockchain, they typically run on centralized servers controlled by the operator, this means that the casino still controls the infrastructure and logic, even if results are verifiable after the fact.

Seed and game logic are also stored on a private infrastructure, there is no public ledger or immutability guarantee, the operator can technically delete or overwrite logs unless independently monitored.

Unlike blockchain-based systems, there are no third-party validators like miners confirming the validity of games: All game results, seed and verification tools are issued by a single source of authority: the platform itself.

The term "provably fair" may mislead users into thinking the system is decentralized or tamper-proof, in reality, the cryptographic proof only protects after-the-fact transparency, not

real-time decentralization, this creates a surface-level fairness, not one embedded in system design.

Chapter 3: The Role of Blockchain in Addressing Trust

3.1) Brief introduction to Blockchain Technology

Blockchain, when decentralized, is an immutable digital ledger, basically a database where transactions (most commonly), but also data, is stored in a chain of blocks (that's where the term blockchain is derived), each block is cryptographically linked to the previous one, once a block is added it cannot be modified without the consensus of the network.

Compared to a traditional database (e.g., MySQL), the main difference lies in its control; traditional databases are centrally controlled (in our case by a casino or tech provider), blockchain, on the other hand is distributed among multiple nodes, which all share responsibility and prevent unilateral control, this makes decentralized blockchain both transparent and tamper-proof.

A decentralized database (if validated by independent nodes, e.g. Bitcoin miners) completely removes the need to trust central authorities, in our case, transactions, seed generation or even full game logic can be made public, visible and auditable.

In simpler words, it offers an infrastructure for trustless interaction, aligning closely with the goals of PF systems.

There are 3 core features that blockchain has that support trust:

1) Decentralization: no single party controls the data or the outcome.
2) Immutability: once recorded, data (e.g. game result, seed hash) cannot be altered.
3) Transparency: anyone can view the record and verify the integrity.

Smart contracts, along with blockchain technology can be used to grant fairness in crypto casinos.

Smart contracts are self-executing pieces of code deployed on a blockchain, in our case they can be utilized to grant automation in games like Dice or Roulette, making sure rules are applied without human intervention, in simpler words, they guarantee outcome logic runs exactly as written (granted that the code is bug-free and transparent).

While blockchain runs cryptocurrencies, its potential in gambling goes beyond deposits and withdrawals, it can host verified randomness, public records of game rounds and trustless payout mechanisms.

3.2) Blockchain Use in Crypto Gambling platforms

In the majority of crypto casinos blockchain is limited to deposits and withdrawals, transactions are fast, borderless and support a wide variety of blockchain networks; however, this use is financial, not related to fairness or randomness.

Despite the association with blockchain, most PF mechanisms run off-chain, this means that these algorithms run entirely on the platform's private backend, this means that nonce, server seed generation and result computation happen off-chain, on centralized servers.

Platforms like Stake.com and BC.game use PF, however, without full decentralization the system cannot be considered completely trustless

True on-chain gambling would require hosting the game logic on smart contracts. This approach exists only in relatively small projects (e.g., Ethereum or Arbitrum-based dApps), and not on major platforms like Stake.com. In practice, most PF casinos prioritize user experience, speed, and scalability over on-chain.

Most platforms are not fully on chain, as full on-chain execution is more expensive and slower, due to network fees and congestion.

Furthermore, full transparency might limit flexibility in game development and design, the average player also rarely demands or understands full decentralization, therefore platforms mainly focus on branding.

Some Web3-native platforms (e.g. BetSwirl) explore on-chain randomness and the use of smart contracts, however they remain marginal compared to mainstream crypto casinos.

3.2.1) Polymarket and the Liquidity Problem

Despite the slow adoption of fully on-chain gambling systems, Polymarket remains the most popular and widely used decentralized prediction market in the blockchain ecosystem. Unlike most crypto casinos that operate off-chain with provably fair mechanisms, Polymarket executes its logic entirely via smart contracts and relies on decentralized oracles for outcome resolution. It represents a real-world benchmark for what fully transparent, blockchain-native betting can look like.

Built on the Polygon blockchain, Polymarket lets users wager on real-world events (e.g. who will be the next Pope); markets are governed by smart contracts and resolved via decentralized oracles (bridges that connect smart contracts on a blockchain to real-world data and external systems).

Users can view all trades, odds, liquidity and outcomes fully on chain, this is a true example of transparency and decentralized betting.

All rules are enforced by smart contracts, outcomes are settled automatically once an oracle posts the result, no centralized operator sets odds or holds funds, bets are pooled and managed via liquidity mechanisms.

This overall sounds great, however full on-chain decentralization has a main bottleneck, liquidity.

Niche or complex markets often suffer from low trading volume, wide bid-ask spread and high slippage on larger trades, this strongly limits the size of the bets and affects the reliability of odds.

Without enough liquidity, decentralized platforms can't offer the same UX as centralized casinos.

The Polymarket case highlights how a lack of significant user engagement and capital can prevent a technically fair system from achieving practical usability.

3.3) How Blockchain Addresses the Core Limitations of Provably Fair Systems

While provably fair mechanisms rely on cryptographic tools to ensure transparency, they still depend heavily on centralized infrastructure and user trust. Blockchain technology, when properly integrated, can directly resolve several of the key weaknesses identified in Chapter 2.

The table below compares six core problems identified in Chapter 2 with blockchain-based mechanisms that could resolve them.

Blockchain-Based Solution	**Problem Solved (from Chapter 2)**
Immutable storage of seeds and outcomes	Hidden values, unverifiable backend logic
On-chain smart contract execution	Dependence on centralized servers
Use of verifiable randomness (e.g., Chainlink VRF)	Doubts about randomness and seed generation
Automatic, trustless payouts via smart contracts	Delayed, rejected, or manipulated payouts, scam websites
Hardcoded and auditable house edge logic	Opaque or variable house edge (e.g., in Dice)
Decentralized governance via DAOs	Centralized control and lack of user input

As the table shows, blockchain doesn't just offer theoretical improvements, it introduces architectural changes that shift fairness enforcement from centralized platforms to open, verifiable systems. However, almost no major crypto casino currently implements these principles.

Blockchain's unique combination of immutability, decentralization, and programmability enables it to address key weaknesses of Provably Fair systems more effectively than conventional solutions.

As an example, consider the immutable storage of seeds and outcomes. As previously stated, traditional approaches might rely on server logs or third-party audits to record game data, but these methods can be altered or deleted without user knowledge. In contrast, storing game outcomes and seeds on a public blockchain ensures that no party: neither the operator or a third-party auditor, can modify the data retroactively. The hash of the seed, once published on-chain, becomes tamper-proof by design.

Another clear advantage of blockchain technology is in trustless payouts; in centralized systems, payouts depend on the operator's integrity; users must trust that their winnings will be honored. Even with legal contracts or escrow systems, execution is subject to delays or disputes. With blockchain, smart contracts can encode payout rules directly on-chain. Once triggered, the contract executes autonomously, with no need for human intervention, legal enforcement, or third-party arbitration. This minimizes friction and removes the possibility of withheld or manipulated payouts.

In short, while traditional cryptographic methods enable verification, only blockchain can enforce fairness by design through public transparency and self-executing logic.

Chapter 4: Business, Market and Future Dynamics

4.1) Real-World Examples: Stake.com and BC.Game

To better understand how provably fair systems and blockchain are applied in practice, this section analyzes two of the most prominent crypto gambling platforms: Stake.com and BC.Game. While both claim to offer transparency through provably fair mechanisms, their actual implementations reveal important differences and limitations in terms of decentralization, user control, and blockchain integration.

Stake.com allows users to verify each game result using server seed, client seed and nonce, the server seed is hashed before gameplay and revealed afterward for verification, players can change the client seed, but this option is somewhat hidden in the UI and resets periodically.

Verification tool is hosted by the platform, results can be verified through the on-site tool, however there is no blockchain logging, no third party auditing and no use of public smart contracts; blockchain is limited to payments, game logic runs entirely off-chain and is fully controlled by Stake's servers, randomness is also internal and not backed by systems like Chainlink Verifiable Random Function, therefore trust still fully relies on Stake's internal backend.

BC.Game on the other hand is claimed to be a more transparent crypto casino, it offers similar PF based on seed hash commitment and client input, documentation is more open than Stake's and includes technical references in their whitepapers.

Players can manually input client seeds and fairness verification tool is provided with visual breakdowns of each component in the seed-hash system.

Despite better documentation, game logic still runs off-chain and there is no use of smart contracts; users are encouraged to verify, and guides exist, but the system still relies trust on the backend.

In conclusion, both Stake.com and BC.Game encourage users to verify game results through on-site tools, and while their full backend code isn't open source, the verification logic is transparently documented. This has allowed the community to replicate and audit it through third-party open-source tools, freely available on GitHub, reinforcing trust through open validation, even without full platform-level code disclosure.

4.1.1) Sponsorships, Ownership, and Influence: Stake.com and Its Competitors

Beyond the technology and user experience, Stake.com's rise has been powered by aggressive sponsorships, celebrity endorsements, and a global expansion strategy. This section explores who controls the platform, how it built its image, and the controversies it has faced, comparing it with other major crypto casinos in terms of transparency, marketing, and regulatory exposure.

Stake.com, originally founded in 2017 by Ed Craven and Bijan Tehrani, is a privately owned company with ownership equally divided between the two founders.

Ed and Bijan were also the founders of Primedice (Stake's predecessor), Primedice was created in 2013 as the first cryptocurrency gambling platform, the website was a success from the start, this led to an expansion and to the creation of Stake.com; to this day Primedice is still active and owned by the two founders, the website has no regional limitations, contrary to Stake.com where players in Italy and other countries cannot access the platform.

Stake.com is licensed in Curaçao, an Island located about 100km north of Venezuela, it is an autonomous country within the Kingdom of the Netherlands, historically the country has been known to provide easy access to online gambling licenses, thanks to the presence of 4 Master Licensors.

Stake operates under Easygo, an Australian tech company, however it operates globally through offshoring and local entities.

Many concerns have been made about the integrity of the business, specifically about their headquarters in Curaçao, many people have been skeptical on how a multi-million-dollar company has their headquarters in a small, 1-floor building.

Stake.com has mainly gained trust through its sponsorships, the most notable being the one with Drake, with a +100-million-dollar contract and endorsements with streamers, other notable sponsorships include the one with Everton Football Club, UFC, Alfa Romeo F1 team and influencers like xQc, who reportedly generated $119M in bets.

Until 2022 crypto-gambling streams were promoted on Twitch, until the terms of service were changed to have a stricter approach towards crypto-gambling.

This led to the creation of Kick.com, co-founded by Ed Craven along with other partners linked to Stake's infrastructure and marketing campaigns.

Stake does not officially own Kick; however, Kick's staff and moderation team largely overlap with Stake's ecosystem, additionally, streamers like xQc and Trainwreckstv, who previously promoted Stake were among Kick's first big names; this matters as Kick allows Stake and other gambling platforms to retain visibility in front of massive online audiences.

In its early days, Stake.com could be accessed via VPN, even from countries where the platform was officially banned/restricted, this allowed users to bypass geolocation blocks and gamble using only a crypto wallet and minimal verification. The platform has now closed this loophole, but it was still active during Stake's major growth phase and raised major concerns about regulatory evasion.

Stake's marketing strategy included paid partnerships with online streamers, most notably Adin Ross, xQc and Trainwreckstv, these streamers promoted crypto gambling to audiences that often included underage viewers; critics argued that this normalized high-risk gambling behavior among young, impressionable fans was ethically questionable.

Furthermore, a UK media investigation tested Stake's KYC system, where, a journalist created an account and gambled for over 48 hours using a photo of a Strepsils lozenge box as fake ID, this showed that the platform identity checks were inadequate and could be bypassed with minimal effort, the incident became public and prompted scrutiny into Stake's compliance with AML and underage access rules.

In response to growing scrutiny, Stake has begun investing in legal and compliance infrastructure, the company has hired dedicated compliance teams, legal advisors and regional managers in key markets, additionally, Stake has started pursuing gambling licenses in stricter jurisdictions, shifting from Curaçao's minimal regulations to more robust frameworks, examples include new market entries (or attempts) in Italy, Portugal, Colombia and the UK (briefly via Stake.uk.com, now defunct).

These efforts show a strategy to legitimize operations in regulated regions and diversify from its Curaçao -only model.

The creation of Kick is also seen as part of Stake's rebranding ecosystem. Kick serves as a marketing channel but also positions itself as creator-friendly, offering more fair revenue splits compared to Twitch and looser streaming rules.

Stake's model is not unique. Other major crypto casinos such as BC.Game, Rollbit, Duelbits, and BetFury adopt similar approaches but differ in how they handle regulation, transparency, and promotion.

BC.game, founded in 2017 has also had major sponsorships, the most notable ones being with Leicester City Football Club and with the Argentina National Football Team, the company also faced license issues in Curaçao and, after a bankruptcy case moved their operations under a license from Comore, an independent nation located in an island at the north of Madagascar, the company still operates largely offshore.

Rollbit, launched in 2020 has a quite unique structure, mixing casino games with crypto trading (NFT's, crypto futures) main sponsorships include SSC Napoli and FaZe Clan (the biggest e-sports organization), the company has faced severe backlash for removing license information from its website in 2023, causing panic over regulatory status, firm claims to be licensed in Curaçao but it's vague about jurisdiction details.

Duelbits, a smaller platform has also made some key sponsorships such as the one with Aston Villa Football Club and Conor McGregor, they mainly rely on white label licensing (company operates its gambling website under another company's gambling license, typically a firm that already holds a valid license in a strict jurisdiction, such as the UK or Malta) to enter into restricted markets, the company is less exposed than Stake or BC.game but faces similar legal risks and challenges.

BetFury on the other hand has had no major sponsorships, as it focuses on a token-driven community via its native coin (BFG), which earns users a share of the platform's profits, it is

viewed as more ethical however it still operates under a Curaçao license and allows VPN access in restricted areas.

4.2) Remaining Challenges and Future Potential of Provably Fair and Crypto Gambling

While blockchain and provably fair systems have introduced new standards for transparency in online gambling, the industry still faces major challenges related to usability, regulation, and mass adoption. At the same time, new technologies and models offer potential to reshape how fairness is implemented and perceived.

One of the main challenges of this evolving sector is limited user understanding, as most players don't verify outcomes, this is due to the verification process being too technical and often hidden behind poor UI, this leads to an underuse of PF, even when available.

Additionally, most crypto-casinos still run off-chain and game outcomes are still computed on centralized servers, this limits the use of blockchain strictly for payments, not gameplay.

Another important factor is the current lack of regulation and standards, as there is still no global legal standard for PF implementation, this leads to a potential misuse of the label "provably fair" for exclusively marketing purposes.

Lack of security and KYC also raise both legal and ethical concerns, as systems remain vulnerable to fraud, VPN's and fake ID's, hacks are also a major concern, as Stake's $41M theft reveals crypto casinos' security flaws.

Today the market still strongly relies on branding, as players are more influenced by streamers and sponsorships than by fairness tools, currently, PF remains a niche trust mechanism, not the main driver of reputation.

Despite these limitations, the evolution of provably fair systems and blockchain technology presents meaningful opportunities for the future of online gambling.
For example, the adoption of on-chain game logic could be achieved with the use of smart contracts, public game logic could lead to completely trustless platforms, removing server-side manipulation risks, platforms like Polymarket are early examples, more could follow.

Decentralized randomness, such as Chainlink VRF could replace proprietary RNGs with publicly verifiable randomness, increasing trust and remove control from the operator.

User education could also be better implemented, such as better tutorials and user-friendly open-source verification tools could help users to actively verify results.

Furthermore, countries may adopt standards requiring verifiability on smart contracts, legal pressure may push platforms to shift from offshore to more regulated markets.

The most important step, however, could be integration with Web3 identity and wallets, future PF platforms could use decentralized identity (DID) to simplify KYC.

Players could verify games with user-friendly open-source tools, while platforms could verify age requirements using zero-knowledge proof, replacing invasive KYC checks and enhancing privacy.

Chapter 5: Beyond the Algorithm – A View from Inside the System

5.1) My Perspective on Provably Fair Gambling

After analyzing how provably fair systems work and how they are implemented across major platforms, this section presents my personal view on their actual impact. While the concept is mathematically sound, its practical relevance in the current gambling ecosystem is far more limited.

In theory, PF eliminates the need for trust, in practice, however most players still trust the brand, not the cryptographic principle.

Mathematical transparency, though crucial, remains largely inaccessible to the general public. This issue is compounded by popular cryptocurrency gambling live streams, like those featuring Trainwreckstv or Adin Ross, where results are never verified in real time.

As a result, most spectators, particularly those who aren't tech-savvy, lack the means to confirm the fairness of these outcomes; additionally, platform UI/UX rarely encourages or teaches users to verify outcomes.

This leads to a result where fairness becomes a backend feature, while front-end trust is built through sponsorships, influencers, flashy designs and big promotions (eg. Casino bonuses).

From the average user's perspective, "Provably Fair" is just often a label, not a functional tool.

As someone who has studied this system in depth, the concept has massive potential, but the current reality feels underdeveloped and underutilized.

PF is a credibility tool, but effective only when users know how (and why) they use it, without both education and intuitive design the math becomes invisible, shifting trust back to branding.

5.2) Why Adoption Remains Limited

Despite the technical promise of provably fair systems and decentralized gambling, their adoption remains limited. This section explores the reasons behind this gap, including user behavior, platform incentives, and the continued dominance of traditional gambling operators in regulated markets.

As previously mentioned, the vast majority of crypto gamblers follow convenience and reputation, not code.

On the other hand, traditional online casinos (such as Sisal, LeoVegas, Lottomatica...) still dominate regulated markets (e.g. Italy), limiting PF platforms visibility.

These regulated operators benefit from legal approval, brand familiarity and complete fiat compatibility, as you could go to a Sisal center and bet using cash, not virtual money.

Decentralized platforms such as Polymarket still face major friction, due to wallet setup complexity, no fiat adoption, thin liquidity outside major events and complex/unfamiliar interfaces.

Regulatory gaps allow centralized platforms to operate almost as a “Black box”, with minimal transparency, and almost none are pressured to adopt PF standards.

At the same time, if regulation fails to adapt, crypto gambling is likely to grow further:

For example, fiat gambling through platforms like Sisal is tracked by banks, which can affect loan eligibility or credit scores, with crypto gambling the same behavior remains off the radar, not less risky, but less visible.

This regulatory loophole incentivizes users to gamble via crypto to avoid financial consequences, this is something I personally find inconsistent, as crypto gambling is still gambling, just harder to trace.

5.2.1) Stake.com vs Polymarket – A Comparative Overview

To better understand why provably fair systems and decentralized gambling haven't achieved widespread adoption, it’s useful to compare two of the industry's most well-known platforms: Stake.com and Polymarket. While both operate in the crypto space, they represent very different models — one centralized and entertainment-driven, the other is decentralized and information-based. This section outlines their differences in performance, perception, and structure.

In terms of economic performance, Stake.com revenue jumped from $2.6 billion in 2022 to 4.7 billion in 2024, with a regular user base of ~600,000, with a big share of users located in Asia and LATAM, with a massive spending on marketing and endorsements.

Polymarket on the other hand had a monthly trading volume peak at 2.5 billion, during the US elections, then it stabilized at 1.1 billion, the company is currently valued at 1.1 billion (2025).

The company’s revenues come from a 2% fee on net winnings, the company doesn’t profit directly from user’s losses, in 2025 the active user base was of ~236,000, while the historical traders are ~1.2 million.

Stake.com became widely recognized due to celebrity/influencers campaigns and is trusted for big payouts and slick UX, but sometimes criticized for possible game manipulation, there are frequent user complaints on Trustpilot; mainly about rigged games and blocked withdrawals (we can’t be certain about the truth on this).

Polymarket on the other hand is viewed as transparent and decentralized, bets are settled via smart contracts, their market is praised for accuracy (for example, 2024 election forecasts

outperformed polls); criticism has also emerged, due to potential insider market manipulation, such as whales skewing low-liquidity markets.

Stake's business model is a centralized, off-chain gambling platform, with cryptocurrencies used only for deposits and withdrawals, company makes profit from house edge and sportsbook margin, like traditional casinos

Polymarket on the other hand works with decentralized peer-to-peer prediction markets, trades happen via yes/no tokens on Polygon, all outcomes are resolved by oracles, in their market model there is no "house", and profits are earned from trading fees and liquidity-based activities.

Stake is privately owned by it's founders, there is no community governance and strategic control remains highly centralized.

Polymarket operates from NYC, currently the company is restricted in the US after CFTC fine, there is no DAO/token governance, decisions are centralized but the code is decentralized.

Stake's strengths are a massive variety of games, fast UX and global liquidity, along with a strong VIP program, affiliate system and 24/7 entertainment value.

Weaknesses include questionable legality in some markets, historically weak KYC, centralization (historically led to user ban and loss of deposited funds), and ethical-based criticism (such as influencer marketing to underage viewers e.g., Twitch ban).

Polymarket's main strength is having a fully on-chain, transparent and trustless platform, with markets related to real world events (politics, sports, crypto), unavailable elsewhere.

"Wisdom of crowds" effect makes odds data-rich and potentially insightful; in 2025 there has been a partnership with X (former Twitter) for AI generated prediction feeds.

Weaknesses include thin liquidity in less populated markets (wide spreads = poor odds), alleged manipulation by high rollers using multiple wallets, low user retention rates (especially after US elections), and unclear regulatory status in several countries like France and Singapore.

In conclusion, while Polymarket offers a more transparent and decentralized model, Stake.com's significantly higher economic performance and user base suggest that most gamblers still prioritize convenience, variety, and brand recognition over verifiability and decentralization. For now, the market clearly rewards entertainment over transparency.

5.3) What Would a Truly Fair System Look Like

While many platforms use the label "provably fair" as a marketing tool, very few offer true end-to-end transparency. This section outlines what a genuinely fair crypto gambling system would require, from game logic and randomness to user interaction and governance.

A truly fair system would require full on-chain logic, all games outcomes should be computed and executed by smart contracts, not centralized servers, this removes the need for trust in the operator as it would not be possible to manipulate the backend.

Code shall be open source, both game logic and verification tools should be public and auditable, with third parties able to validate fairness independently.

Random functions should also be verifiable (e.g. Chainlink VRF), instead of proprietary RNGs, this makes players able to verify that outcomes are unpredictable and not tampered with.

Additionally, players shouldn't need to deposit funds into a custodial balance, all bets would have to be placed directly from wallets with the use of smart contracts.

Platform's commissions, edge and liquidity spread should be disclosed and fixed, in order to prevent hidden odds manipulation, furthermore the house edge/commissions would have to be as low as possible, just enough to reward network verifiers.

Furthermore, the platform should be governed by DAOs or by token-based voting, to decide what games to launch, platform rules, oracle/data dispute resolution.

Age/KYC verification shall use ZKP, and have only an age requirement, this solves legal compliance issues without centralizing user data.

Finally, the platform should actively teach users how to verify outcomes, and verifiability would need to be easy, intuitive and emphasized.

5.4) My Final Thoughts

After analyzing both the technical and practical aspects of provably fair systems, as well as their real-world adoption, I believe the current models only scratch the surface. In this section, I share my personal view on how these systems could evolve to better align with the values of decentralization, transparency, and user empowerment.

Provably fair systems are an impressive innovation, but remain underused in practice due to user inertia, poor education and platform incentives.

Despite the existing challenges, the rise of platforms like Polymarket shows that there is a genuine appetite for alternatives to traditional betting, especially when linked to current events, data and transparency.

In my personal view, the future lies in hybrid models that combine the decentralized architecture of Polymarket with the entertainment value and variety of games seen on Stake.

A new kind of platform should emerge, where users don't only bet on real world events, but also play fully on-chain minigames, such as dice, crash, blackjack; all built with the features listed in chapter 4.3.

This would turn games into peer-to-peer experiences, not house-driven profits.

I also believe regulation should play a strong role in enforcing transparent PF algorithms in already existing systems, all platforms should be required to make outcome verification accessible, transparent and auditable, users can and will care about transparency, but only if platforms invest in education and UX/UI; better interfaces, tutorials and open tools are needed to bridge the gap between trust and understanding.

From my perspective, trust is the main issue: many platforms, including major ones like Stake have demonstrated unethical behaviors, from opaque bans to aggressive marketing towards minors, this lack of integrity makes centralization a liability.

In the end, the greatest challenge isn't technological, it's ethical. Many traditional and crypto gambling platforms have chosen manipulation over fairness, prioritizing profits over transparency. The next generation of platforms must reverse this logic, building systems that serve their users with integrity, clarity, and verifiable trust.

Chapter 6: Conclusion and Reflections

This chapter summarizes the main findings and offers personal reflections on where crypto gambling is headed and what a fairer future could look like.

This thesis investigated how provably fair systems work in crypto gambling, with an analysis of both real platform implementations and the gap between theory and practice.

We conclude that PF is not revolutionary if the system isn't truly independent and transparent and that most platforms implement PF superficially or in ways that common users can't easily verify.

Polymarket, with its different structure and business model, is the only platform that feels genuinely fair and decentralized, however some concerns are still present, more specifically about liquidity manipulation and insider influence.

The ideal future model for a completely fair platform is a fully trustless and decentralized platform with transparent fees and open-source smart contracts, with gameplay handled without custodial deposits.

Today's centralized platforms such as Stake exploit users through vague odds. Influencer promotions and opaque processes, real fairness is rarely achieved in practice.

My view is that traditional platforms such as Sisal or Bet365 will likely resist PF adoption but may eventually integrate it to stay competitive, in the next 5 years centralized giants will still dominate, a shift toward fairer systems may require 10+ years.

Regulation in 2025 is still underdeveloped, in my opinion enforcement of PF standards is necessary for user protection and market credibility.

Future research around this topic could be related both to the psychology behind the success of platforms like Stake and to the potential applications of PF outside gambling, such as video games, giveaways and more.

My final vision is that the future of gambling shouldn't just be profitable, it should be ethical, transparent and user-first, platforms must move from manipulation to empowerment, earning users' trust by design, not marketing.

Bibliography (APA 7)

Articles & Reports

Cointelegraph. (2025, June 25). *Polymarket set for $200M raise at $1B valuation: Reports*. Cointelegraph. vice.com+15cointelegraph.com+15cryptorank.io+15

Cointelegraph. (2025, April). *Crypto casino profits soar to $81.4 billion in 2024 despite bans*. Chainplay.gg. coincodex.com+11chainplay.gg+11ft.com+11

Pechanga. (n.d.). *Crypto casino revenue hit $4.7 billion in 2024 despite global restrictions*. srnnews.com+14pechanga.net+14cointelegraph.com+14

Yahoo Finance. (n.d.). *Polymarket nears Founders Fund-led funding at over $1B valuation*. en.wikipedia.org+11tech.yahoo.com+11srnnews.com+11

Reuters. (2025, June 25). *Kalshi valued at $2 billion in latest funding round*. en.wikipedia.org+2reuters.com+2techcrunch.com+2

Stake.com Crash/Hack

Vice. (2023, September). *Who pulled off a $41M online casino heist? North Korea, FBI says*. dlnews.com+7vice.com+7businessinsider.com+7

FBI. (2023, September 6). *FBI identifies Lazarus Group cyber actors as responsible for theft of $41 million from Stake.com*. U.S. Department of Justice. en.wikipedia.org+9fbi.gov+9theblock.co+9

Business Insider. (2023, September 8). *North Korean hackers stole $41 million from Stake.com, FBI says*. en.wikipedia.org+9businessinsider.com+9theblock.co+9

SC Media. (2023, September 6). *Over $41M stolen from Stake.com in cryptocurrency heist*. fbi.gov+2scworld.com+2vice.com+2

Platform Profiles

Wikipedia contributors. (2025). *Stake (online casino)*. In *Wikipedia*. deadspin.com+7en.wikipedia.org+7en.wikipedia.org+7

Wikipedia contributors. (2025). *Polymarket*. In *Wikipedia*. techcrunch.com+11en.wikipedia.org+11omniekonomi.se+11

Wikipedia contributors. (2025). *Lazarus Group*. In *Wikipedia*. scworld.com+7en.wikipedia.org+7egr.global+7

Wikipedia contributors. (2025). *Bijan Tehrani (entrepreneur)*. In *Wikipedia*. en.wikipedia.org+4en.wikipedia.org+4forbes.com+4

YouTube & Video Sources

Puppet, G. [@GamblingMadeMe]. (2023, October 6). The puppet of Stake [Video]. YouTube. https://youtu.be/ObDAXqg9O3U

Geraci, N. [@noahgeraci]. (2023, October 2). *Stake.com and the case for better gambling regulation* [Video]. YouTube. https://youtu.be/NXoaBowHE4M