



Whitepaper

(v0.1 October 2023)



Table of Contents

Summary	2
Introduction	3
What is Zeebit?	3
Industry Background	3
The Challenge – Web2 vs Web3 Experience	4
Zeebit’s Solution	6
Platform Overview	8
Stakeholders	8
Original Games	9
Multi-token Betting	9
Additional Application Features	10
Making Web3 accessible for all	10
Economic Model & Revenue Sharing	11
XP System and Reward Mechanisms	14
Governance	14
Zeebit NFTs	14
Technical Overview	16
Why Solana?	16
Smart Contract Structures	16
Security Measures	20
Behind Zeebit	21
Roadmap & Ecosystem Growth	22
Project Roadmap	22
Partnerships and Composability	26

Summary

What is Zeebit?

Zeebit is a decentralized casino powered by a peer-to-peer betting protocol built on the Solana blockchain. The project aims to democratise crypto gambling and displace centralised operators by offering decentralized, transparent and verifiably fair gaming on a platform that combines the best of Web2 user-experience with all of Web3's many benefits.

Zeebit does this through providing a fully on-chain, non-custodial platform that grants players control over their data and most importantly, their assets. Players can play verifiably fair and all-original games directly from their Web3 wallet on Zeebit's borderless and trustless platform.

Community Reward Systems and Ownership

Zeebit incorporates several community reward systems. The platform's benefits and ownership are shared with the community via mechanisms such as a fully on-chain XP (experience points) system, NFTs, unique tokenomics, revenue share, on-chain governance and liquidity provision.

Economic Model & Revenue Sharing

Revenue is generated from a small, mathematical edge on each bet. This consistent revenue will grow with scale and facilitate lucrative revenue share distribution to ecosystem stakeholders. Primary examples of revenue share mechanisms include rakeback, regular bonuses, referrals, liquidity provision and NFT & token staking rewards.

Technical Overview

The Zeebit protocol is built on Solana, which offers the best balance between decentralization, security, transaction costs and speed. It consists of three smart contract types – game contracts, randomness contracts, and contracts dealing with settlement, player profiles and revenue share. These contracts facilitate near-instant bets and almost instantaneous settlement while ensuring security and transparency.

Roadmap and Partnerships

Zeebit's roadmap has three phases:

1. Launch Platform and Enhance Solana User Experience: Platform mainnet launch, early adopter onboarding, NFT project launch, forming strategic ecosystem partnerships.
2. Grow platform and on-board cross-chain players: Launch second generation games, introduce a project token, provide gasless abstractions and cross-chain solutions.
3. Broaden Zeebit's Reach: Launch third generation games, introduce staking and liquidity provision, provide embedded fiat currency on/off-ramping.

Throughout, Zeebit will also seek strategic partnerships with key ecosystem protocols, communities, NFT projects, DEXs and infrastructure providers.

Introduction

What is Zeebit?

Zeebit is a decentralized casino and peer-to-peer betting protocol.

Backed by some of the biggest names in crypto venture capital, and born from the expertise of a Solana-native team, Zeebit is not just another online casino. It's a fully on-chain platform, built entirely on the Solana blockchain.

For the first time ever, players will be able to immerse themselves in a fully decentralized and verifiably fair gaming environment that marries Web3 functionality with a seamless user experience, on par with Web2.

Zeebit promises an unparalleled on-chain gaming experience that is decentralized, permissionless, fair, and above all - fun.

Industry Background

The global online gaming industry services billions of players each year, both online and in land-based gambling establishments - with approximately 4.2 billion people gambling at least once a year¹.

With land-based casinos globally seeing widespread closures due to the COVID-19 pandemic, online gambling is more popular than ever. The global casino & gambling industry was estimated to be worth \$248 billion in 2022². \$90 billion (36%) of that comes from the online gambling industry, which is projected to reach \$370 billion by 2030 at a compound annual growth rate (CAGR) of over 10%³. This astronomical growth continues to be driven by the increasing trend of online gambling, rising legalisation in developing regions, and enhanced internet penetration.

Blockchain technology has started to further accelerate this growth, with clear demand for online gambling platforms emerging in the crypto landscape. In 2023, the Web3 community saw the rise of CasinoFi as a core pillar of the ecosystem.



Two centralized platforms have emerged as worth noting - Stake.com and Rollbit.

Stake.com - Launched in 2017, Stake is one of the earliest centralized crypto casinos. Celebrity partnerships and an early-mover advantage allowed Stake to attract wealthy gamblers across the globe - generating nearly \$2.6 billion in revenues in 2022 alone⁴.

¹ <https://tgmresearch.com/gambling-sports-betting-market-research-in-germany.html>

² <https://www.ibisworld.com/global/market-size/global-casinos-online-gambling/>

³ <https://www.gminsights.com/industry-analysis/online-gambling-market>

⁴ <https://www.ft.com/content/2490279b-9c94-49a8-beff-cbd7c3307586>

Rollbit - Rollbit has over one million registered users⁵ and sees approximately \$40m of betting per day with over \$5 billion in volume wagered by players to date⁶.

However, a number of major concerns arise with centralized platforms:

- **A Lack of Transparency:** All transactions, revenue share and player rankings are processed off-chain, making them unverifiable by the public. A lack of audit documentation and information related to treasury and protocol wallets is cause for concern.
- **Heavy Centralisation:** 76% of RLB token supply is held on Rollbit rather than in user wallets, which poses a significant risk of centralization and potential bank runs. Meanwhile, Stake was famously hacked for \$41m in 2023. These concerns are even more valid when considering the lack of a decentralized governance process.
- **Regulatory Risks:** While licensed, both centralised platforms have major forms of unverifiable revenue share and are used by many users within restricted jurisdictions. This has previously and will continue to invite regulatory scrutiny.

Overall, the platforms mentioned above, and many more of these ‘Web3’ casinos are in fact simply centralised Web2 gaming platforms, enabled by crypto payment rails and a sprinkling of token or NFT utility.

The rise of DeFi and blockchain technology brought the promise that Web3 would democratise everything, but for gambling, the most successful operators are opaque, centralized and profit seeking businesses.

This whitepaper asks the question: Why isn’t the leading experience decentralized, fully transparent and enabled by-and-for its community?

A clear best-in-class, and truly decentralized Web3 gambling protocol has not emerged, **until now**.

The Challenge – Web2 vs Web3 Experience

In this evolving landscape, players face several problems in using traditional Web2 or centralised ‘Web3’ casinos. In many cases these problems don’t surface until a large incident arises. Lacking transparency means problems may not be known to players or to supposed off-shore ‘regulators’.

To highlight some of the key problems stemming from both traditional Web2 and centralized crypto casino platforms:

- A high degree of centralization and lack of transparency;
- Censorship, account limiting and suspension of profitable players;

⁵ <https://tokeninsight.com/en/tokenwiki/all/what-is-rollbit-is-it-worth-the-hype>

⁶ <https://whitepaper.rollbot.com/rlb-whitepaper/>

- Operator ‘credibility’ obtained through purchase of licences from questionable off-shore ‘regulators’, with few levers in substance to protect players from dishonest operators;
- High operational costs which translate to less favourable returns for players;
- Operators and third-party custody firms retaining control over player funds, and little by way of accountability with how those funds are held or used;
- A disregard for privacy and the Web3 ethos of anonymity - often requiring players to disclose significant amounts of information on sign-up or holding player funds to ransom at the point of withdrawal;
- Deposits and withdrawal processes can be slow, and often subject to unexplained delays and restrictions – in some cases, maliciously.

While centralized platforms account for the vast majority of today’s global gambling volume, a truly decentralized Web3 protocol is poised to disrupt this. The fully on-chain nature of a decentralized protocol ensures that players have complete control over their data, assets, and experience. And most importantly, platforms are forced to be wholly transparent and accountable at all times.

Web3 has so much potential to offer players. A fully on-chain platform run on a Solana native protocol enables the following revolutionary benefits for players globally:

- **Negligible Costs and Lightning-fast Transactions:** Unlike on EVM chains, Solana enables players to make lightning fast (sub-second) bets with multiple cryptocurrencies and stablecoins, all at a near-zero cost (~1/100th of a cent per action).
- **Full Transparency:** Every action – by player, platform or protocol – is immutably recorded on the Solana public ledger – providing full transparency to players at all times.
- **Non-custodial and Permissionless:** Frozen funds and censorship are not even a possibility thanks to the non-custodial and permissionless nature of such a platform. Player funds remain in their wallet, and under their control at all times.
- **Secure:** Smart contracts automate, cryptographically secure and authenticate all transactions. Programs can undergo smart contract audits and public attestations by leading Web3 security firms.
- **Borderless and Accessible:** Unlike traditional centralised platforms, which rely on segregated funds tied to particular currencies or jurisdictions, such a platform would operate on a global, immutable blockchain. Players aren’t constrained by their native currencies or the need for banking rails for each region or jurisdiction.
- **Community Ownership & Governance:** Revenue share, project tokens and NFTs facilitate entire communities to participate in the rise of this disruptive change.

- **Innovative Tokenomics:** In addition to playing a role as a betting currency, native tokens can play a role in facilitating governance, revenue share, loyalty programs and other promotional activities – offering wide ranging token utility.

Zeebit's Solution

Operating completely on-chain, Zeebit is the first truly decentralized casino on Solana. It is the first platform across all of crypto that allows players to truly immerse themselves in a fully decentralized and verifiably fair gaming environment by combining the incredible functionality of Web3 with the seamless user experience that players have come to expect from Web2.

Provably Fair and Original Games

Zeebit offers a suite of all-original, fully on-chain games of chance - exclusive to the Zeebit ecosystem. Each and every game is designed, configured and developed by the protocol's core team, ensuring no reliance on third-parties.

The smart contracts powering Zeebit games operate on the Solana blockchain. Verifiable randomness ensures that the result of each and every game is transparent, immutably recorded and provably fair.

A Borderless, Permissionless and Privacy Focused

Connect with your Web3 wallet or social login of choice and dive straight into the action - no tedious sign-ups or personal data mining. Privacy is a core ethos of Web3 and Zeebit upholds that. The protocol does not enforce any requirements to provide information beyond that which players volunteer. Communications and other experience improving features which platforms might offer are entirely on an opt-in basis.

The protocol operates by smart contract transaction on the global, immutable and permissionless Solana blockchain. Funds aren't confined to the borders or speed of regional banking rails, and are free to move across the blockchain in a matter of milliseconds, at any time.

Unique XP System and Reward Mechanisms

Thanks to the on-chain nature of the platform, transparent smart contracts ensure rewards and distributions in perpetuity - eliminating the risks associated with potentially unreliable operators.

Zeebit will feature a unique on-chain XP (experience points) system that allows players to earn rewards, bonuses and benefits as they level up.

Trustless, Non-custodial and Multi-token Betting

Players should not have to place their trust in shady operators or dubious offshore regulators. Nor should they be subject to the often lengthy onboarding processes that comes with them.

Zeebit is fully non-custodial - which means all actions are carried out directly from your Web3 wallet. No deposits are required, and you don't need to trust anyone to hold your assets. Your funds are always in your control - no middleman, censorship or freezing of funds.

Players can maintain their crypto exposure by betting in a range of supported tokens on the Solana network, and can seamlessly swap between different tokens through integrated on-chain swaps.

Combining the Best of Web3 and Web2

Zeebit's user experience is unparalleled in the crypto ecosystem. Players can experience blazingly-fast 400ms game response times, with each transaction costing close to nothing in gas fees (US\$1 can fuel more than 10,000 actions).

Committed to eliminating all user experience hurdles posed by Web3's current implementation, Zeebit is developing 'gasless' solutions - technologies which will completely abstract the concept and cost of gas. These developments will lead to an experience as fast, smooth and simple as Web2, offering players all of the benefits of Web3 - without them even knowing that they're interacting with a blockchain.

Distributed Community Ownership

The success of a decentralized project is driven by the entire community. It's only fair that the benefits of this success, and influence in future successes are distributed across the community too.

Revenue share, project tokens, NFTs and governance mechanisms enable the entire community to participate in the success of the project, and are all part of the Zeebit roadmap.

Emphasis on Entertainment & Fun

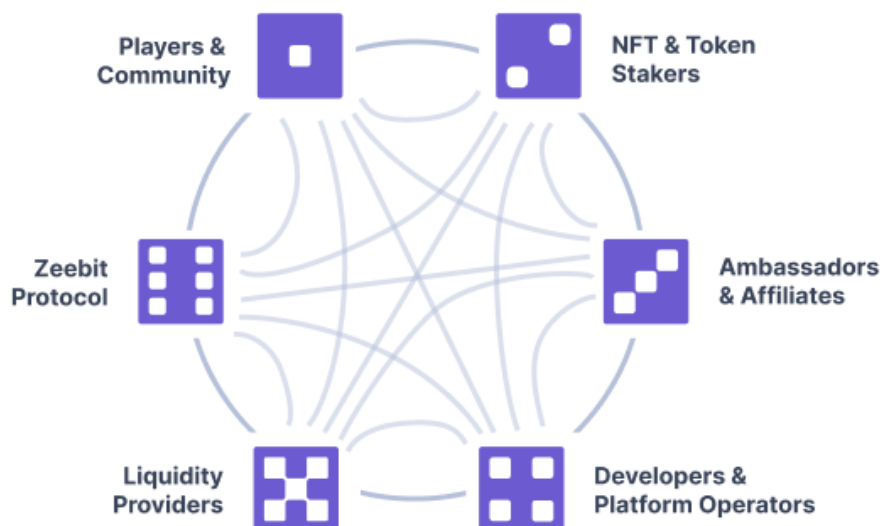
While the benefits of decentralization can't be overstated, Zeebit's emphasis will always be on nurturing a fun and safe atmosphere for its community - one that is built on the pillars of entertainment and amazing player experience.

Ultimately, the Zeebit ecosystem will be supercharged with unique and ever-evolving initiatives, and scope to participate in a multitude of different ways - play, earn, stake - or all of the above.

Platform Overview

Stakeholders

The Zeebit ecosystem has a decentralized, circular economy revolving around community participants, with a range of key roles to play.



- **Players & Core Community Members:** The lifeblood of the Zeebit ecosystem - players enjoy games, win prizes and add life and fun to the community.
- **NFT & Token Stakers:** Stakers receive regular platform rewards, benefits and revenue share for staking their holdings and showing their commitment to the project and the community.
- **Ambassadors & Affiliates:** Players and content creators who help to spread and introduce players and community members into the ecosystem.
- **Developers & Platform Operators:** Other platforms and projects that develop new front-ends and channels to interact with the protocol; in growing their own communities and player base, they help to grow the wider Zeebit community.
- **Liquidity Providers (LPs):** Individuals or entities that stake capital in the protocol's liquidity pools to facilitate betting on the protocol in return for real-yield.
- **Zeebit Protocol:** The core team of contributors and maintainers behind the technology powering the ecosystem, alongside the members helping to execute activities to share and grow the community.

Original Games

Every game on Zeebit will be an original game built by the core team, with no external dependencies on operators or game providers.

The ever-expanding range of games will feature lots of new ways to play, win and earn - all of which are exclusive to the Zeebit ecosystem.

Category	Description & Examples
----------	------------------------

Solo games	It's you versus the liquidity pool! Exciting games with near-instant settlement include Coin Flip, Roulette (solo), Plinko, Dice and Limbo.
Multiplayer games	Win alongside your fellow degens with games like Crash, Roulette (multiplayer) and Slide.
Round or level games	Hold your nerve across rounds with games like HiLo, Tower, Mines or Blackjack.
Jackpot Pools	Winner takes all, or divvy up prizes among other players with jackpot games.
Lootboxes	Create your own, or try to crack open someone else's lootbox to reveal the goods inside.
Lotteries	Check your lucky numbers to see if they've come through - share in pooled rewards and have your chance of winning.
PvP games	Play head-on against a room of other players, or against the whole community with Russian Roulette, exit scam games and more.

Multi-token Betting

Zeebit enables multi-token betting - allowing players to bet, win and earn in a range of Solana (SPL) tokens.



Initially, focus will be on primary ecosystem tokens, major wrapped assets and stablecoins.

As liquidity capacity grows, Zeebit will seek to expand the range of tokens supported - enabling players to bet without giving up their exposure to their favourite crypto projects, or while continuing to collect yield on their liquid staking tokens of choice.

The application will also have several features that enable players to manage token balances and swap between tokens as required - all without leaving the platform's UI.

Additional Application Features

Alongside the array of terrific game experiences, the application will include features to enhance entertainment and in-platform interactions with other players and community members. Features include:

- A live in-platform community chat;

- Integrated NFT utility - set your owned NFTs as in-platform profile avatars, access NFT gated competitions, exclusive features and valuable rewards;
- Leaderboard, with regular competitions and player rankings;
- Shareable betslips - all verifiable on-chain (proof of participation);
- A fully on-chain ambassador and referral program;
- In-app wallet management, with easy-to-use token swapping and token bridging.

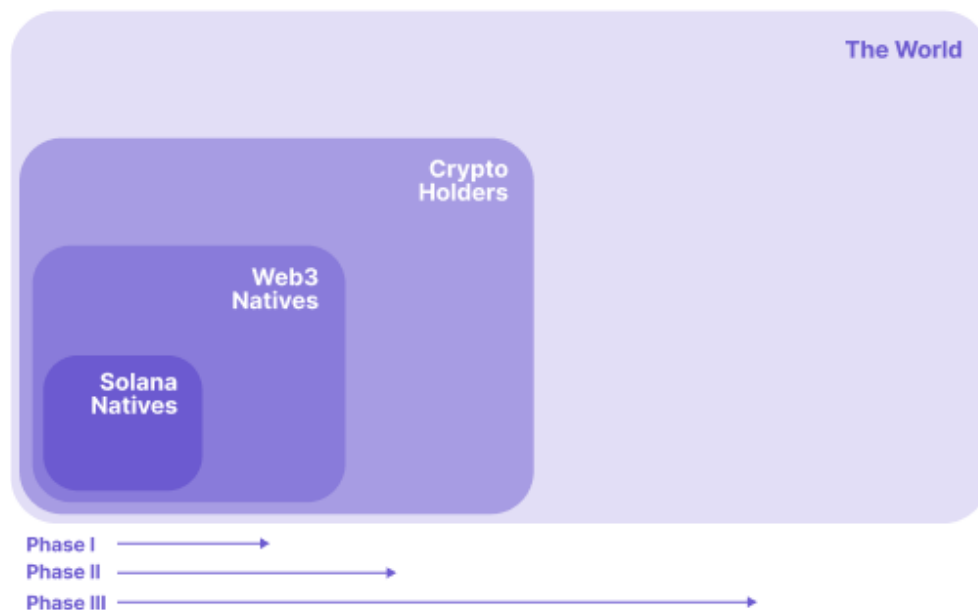
Making Web3 accessible for all



Zeebit.io is built for crypto natives, the wider web3 community, and first-time adopters alike.

The decision to build on Solana was made because of key features unique to the network - all of which enable an uncompromising user experience while achieving all of the benefits and security of Web3.

However, that doesn't mean that Zeebit is constrained to serve only the Solana community. The project's three phase plan, detailed in the Roadmap & Ecosystem Growth section, aims to cater to the entire crypto player base and beyond.



The roadmap sets out a three phase plan which includes (alongside platform, game and community plans) a clear outline of how the user-experience challenges of Web3 vs Web2 will be bridged, making Zeebit accessible to the widest possible audience of players.

Economic Model & Revenue Sharing

As with all gaming platforms, revenue is generated through a small edge taken by the player's counterparty. In the case of Web2 and centralized platforms, this is often referred to as the house's edge. The concept is similar for Zeebit - but with a focus on a more equitable distribution.

With each bet placed, there is a small mathematical edge factored into the game multipliers offered. Over time, and with scale, this edge is expected to generate consistent revenue for the ecosystem.



For Web3 natives, this is analogous to an AMM's (automated market maker) swap fee - a small margin taken to compensate the pool for being a willing counterparty to any trade at any time. Similarly, Zeebit pools are always willing to take the other side of a player's bet.

Unlike a centralized platform - where this edge is simply taken as profit for the operator - the edge on Zeebit is distributed among all of the ecosystem participants through a number of mechanisms.

Not only will Zeebit be the most decentralized and secure platform out there, but also the most generous to its community and ecosystem members. This is thanks to a variety of revenue sharing mechanisms built into the protocol.

Rakeback

Rakeback is a player's share in the expected edge earned on each bet. Players on Zeebit will accrue rakeback for every single bet placed.

Rakeback is determined based on expectancy and not on actual profit-and-loss, so players earn regardless of whether they're winning or losing.

Rakeback rates and earnings increase as players climb the ranks. It's essentially a reward for being an active player and making the ecosystem a fun, interactive and competitive platform for other community members and players alike.

Covering Network Costs

The 'gas costs' associated with covering the Solana network validation are covered by the protocol. Initially, the Zeebit core team developed solutions where the 'rent' (data storage) component of this cost is covered by the smart contract from day one. The team is actively working on solutions to also cover the cost of the entire transaction through instantaneous gas rebates, and in-time, gasless transaction relaying.

Bonuses, Rewards, Free Games, Airdrops & More

On top of direct accruals in the form of rakeback, the platform will feature lots of different ways to win and benefit - surprising players at every turn. Examples include bonuses on key XP milestones and level-ups, random promotions and freebies for community members, airdrops, free participation in side games, and much more.

Core to Zeebit is rewarding active and loyal community members and players. This will be an area of continuous innovation.

Referral Share

Those who help to grow the community by bringing new players into the ecosystem should be rewarded. With every bet placed by a referred player, their referrer will receive a share of the associated revenue.



Many centralized operators pay professional affiliates in proportion to player losses – but this motivates referrers and affiliates to cheer for the wrong side. Zeebit’s revenue share model will reward referrers on an expectancy basis - sharing revenue regardless of whether referred players win or lose.

Those who refer more players, and generate more activity within the ecosystem will also be able to increase the proportion of revenue share they receive. Unlike centralized operators, this is administered entirely via smart contract, allowing referrers and ambassadors to accrue their revenue share mechanically forever.

Liquidity Provider Real Yield

Liquidity providers (‘LPs’) provide the risk capital required to back the entire ecosystem, which covers player winnings on Zeebit games, in return for receiving a major share of each bet’s mathematical edge..

Unlike other elements of revenue share, liquidity providers’ earnings are subject to fluctuations due to the random outcomes of any given bet. On an expectancy basis, they can anticipate a healthy real-yield over time as the platform scales.



Permissionless liquidity provision will be opened up in time, where anyone can play the role of ‘the house’ and earn a real yield from the expected margin.

On Zeebit, liquidity provision is based on single-sided token pools and are therefore not subject to the same risks as typical DeFi liquidity provision. Single-sided token pools and mathematical edge means providers earn a real-yield (as opposed to synthetic incentives common-place in DeFi) and are not subject to impermanent loss.

Platforms & Independent Front-ends

Platforms which promote and offer ways for players to easily interact with the protocol can operate independently of the protocol and liquidity powering it behind the scenes. Initially, the Zeebit project will develop a core platform and decentralized application ('dapp') user-interface to interact with the protocol.

Over time, the Zeebit ecosystem will seek to encourage and incentivize independent platforms to build new ways to interact with the core protocol, and to tap into shared liquidity pools. Platform developers will participate in revenue share for developing, promoting and operating these channels and sub-communities within the ecosystem.



Examples might be platforms that cater to particular regions, languages or gaming niches, or NFT communities that offer their own gaming platform - with collection themed games, or wagering in their own project currency.

NFT & Token Stakers

Once the Zeebit token is launched, token & NFT stakers will be rewarded for securing the protocol by participating in revenue share distributions. Details on the exact mechanisms, levels of participation and additional benefits to stakers will be provided closer to token launch.



Rewards will be available for all stakers, but will have a particular emphasis on rewarding those most loyal and committed to the longevity of the project.

Zeebit Protocol

In order to keep the protocol humming, ship new features, and provide a world class decentralized experience, the protocol will collect a share of revenue which will continuously improve the project.

XP System and Reward Mechanisms

Zeebit offers a fully on-chain XP (experience points) system like no other - climb the ranks as you play and enjoy the bonuses, benefits and rewards that come with it. We don't just celebrate winners or compensate losers, we reward players for every bet they take - regardless of the outcome.

XP is also awarded for different actions and involvement in the platform and community along the way - like referring new players, active participation in the community or competing in ecosystem challenges and quests.

Players climb ranks as they reach XP milestones, and unlock more and more benefits and rewards.

XP will also be a key criteria in eligibility for major project events like token launches, NFT drop whitelists, airdrops, and benefits from partner projects.

Governance

Staying true to the project's decentralized and permissionless ethos, community members will have a chance to have their say in the direction of Zeebit through distributed project governance. To prevent manipulation and to ensure governance represents those with the project's best long-term interests at heart, only staked token holders will be eligible to participate in voting.



More information on the exact format of project governance will be provided in time.

Zeebit NFTs

A limited edition NFT collection will be launched alongside Zeebit's mainnet debut. The collection will offer early community members a chance to utilise within the ecosystem of Zeebit & receive rewards upon the success of Zeebit. .

The collection will feature several different forms of utility for early adopters, including in-platform benefits, exclusive features, access to future milestone events and whitelists, and access to platform revenue share – ensuring that the collection remains central to the platform and protocol, and retains value over time.



Details of the collection are under wraps, but will be teased as the launch date approaches.

Technical Overview

❑ This section contains a number of sections of technical detail containing terminology related to blockchain technology, cryptography and verifiable randomness which may be unfamiliar to many readers. Effort has been made to distil the information but many of the concepts are inherently technical in nature.

The Zeebit platform is completely powered by the Solana native Zeebit protocol - designed and built by the project's core team.

Why Solana?

Solana remains the most promising layer one (L1) chain in terms of the balance between decentralization, security, transaction costs and speed. Zeebit set out to build a protocol which, for the first time, would offer players all of the much needed benefits of Web3, without compromising on the experience they've come to expect from centralized, Web2 platforms.

Solana's 400 millisecond blocktime enables near-instant responses, and immediate, non-custodial settlement, directly to a player's wallet. And all of this can be achieved for a cost of approximately \$0.0001 per bet!

❑ Soon, players won't even incur the ~\$0.0001 gas cost, thanks to developments underway in gas abstraction, gas rebates and ultimately gasless transaction relaying.

Solana's block capacity also ensures that there is plenty of room for growth, meaning scaling won't be a challenge. Current estimates put Solana's transaction capacity at 50,000 - 65,000 transactions per second.

Smart Contract Structures

The Zeebit protocol consists of a number of constituent smart contracts, each servicing a key function. Solana's cross program invocations (CPI) enable these contracts to speak to one another in a secure way and request that they carry out their respective roles in a modular way.

The module approach enables a number of key benefits:

- Separation of functionality makes the programs easier to maintain and develop

- New games and features can be developed and easily integrated into existing contracts which handle core functionality like providing verifiable randomness, player settlement, updating statistics and distributing revenue share.

Game Contracts

Every game is different - some more than others. Game contracts allow for specifying and configuring the rules of various games that will be provided by the protocol. Many game variants can be supported by different configurations and rulesets within the same contract, while others may require entirely standalone instances of contracts.

Game contracts handle initialising requests for new game instances triggered by players, or scheduled by set intervals. These contracts make automated decisions on whether bets can be accepted based on pre-specified criteria or rules, and determine the multipliers or payouts that should be offered based on a player's requested game configuration or bet selection.

When provided with verifiable randomness (see below), the smart contract converts generic random inputs into meaningful game results, and assesses bets to determine whether they've won or lost. It also determines what transfers should be made to settle these bets.

Randomness Contract

Provision of verifiably fair randomness is core to the ecosystem.

On-chain randomness might sound easy to implement, but it's quite the opposite. If implemented incorrectly, dishonest developers could exploit players, or savvy players could game the system and drain liquidity providers of their funds.

The deterministic nature of the blockchain means that certain aspects of randomness must be sourced from off-chain. Achieving this in a way that is secure and verifiable is crucial.

Zeebit's solution involves leveraging the same zero-knowledge cryptographic verification that is used by Solana's runtime - a solution core to the whole blockchain, and one which has been entrusted with over \$10 billion at its peak⁷.

There are four ingredients to Zeebit's verifiable randomness, each playing an important role:

- **Client seed** - a value provided by the player when placing their bet, which can be changed at any time (it could be changed for every single bet, for example) prior to a bet being placed;
- **Request nonce** - an ever monotonically increasing number incremented each time a request was made - providing entropy and ensuring that it is impossible that an identical set of seeds could ever occur;

⁷ <https://defillama.com/chain/Solana>

- **Future blockhash** - at the time the request is created, the contract will specify that a particular future blockhash must be used. The earlier blockhash that can be used (for instant bet requests) relates to the block of the current request transaction. This blockhash, along with any future blockhash is by definition unknowable to anyone at the time it is requested.
- **Provider's secret key** - the hidden off-chain ingredient. A randomness provider node has an address on the blockchain and maintains a secret key to operate this address (the same way any Solana wallet does). When the provider node receives these ingredient seeds, it concatenates them into a byte array of fixed length and signs the message with its secret key, producing an unpredictable outcome - the randomness.

The off-chain provider submits a transaction to the randomness smart contract, which in turn invokes a callback to the relevant game contract once the response has been validated against the request.

Using the same cryptographic toolkit leveraged by Solana's runtime (Ed25519 Signature Algorithm), anyone can independently prove or verify that randomness provided by a given provider was produced without the seeds having been tampered with.

- Players can validate that the client seed used was indeed the seed which they provided;
- The monotonic increasing of the randomness contracts request nonce is visible all-times on Solana's immutable ledger;
- The blockhash corresponding to the pre-specified slot number in the request can be retrieved from Solana's immutable ledger;
- An implementation of the Ed25519 verify method in any programming language can be used to provide a zero knowledge proof (i.e. without revealing the secret key) that these seeds, and only these seeds, were signed by the secret key corresponding to the stated provider's public key - without any tampering whatsoever.

The platform interface will facilitate ease of verification of this and all of the elements of randomness generation are published to Solana's immutable ledger, for anyone to validate at any time.

Settlement, Profiles & Revenue Share Contract

The last of the core smart contracts deals with settlement of funds, maintenance of on-chain state like profiles and ranks, tracking statistics and handling revenue share distribution.

Think of it like an automated, ecosystem-wide teller that enables pool and protocol funds to be moved around in accordance with pre-specified rules – all without the ability or need for any influence from individuals or organisations to authorise any given transaction.

When the game rules have been applied and the conditions of a bet accepted by the game's contract, an invocation is made to this contract requesting that the

appropriate transfers take place to fund the bet and to place a temporary hold on the amount that might be paid out to the player should they win. The contract dynamically determines if the pool has sufficient funds to take on this bet, and that it is within an acceptable range.

After randomness has been provided and the game has performed and assessed each bet, it invokes this contract once again, requesting that it settle the bet as required. Funds are settled directly into the player’s wallet in the event of a win, or the temporary liability and player wager can be released and made available for future wagers in the event of a loss.

The contract also updates various elements of state - keeping track of key player, platform and ecosystem metrics and statistics – like volumes bet, won and lost. It determines XP, rakeback and revenue share across all of the different ecosystem roles and distributes this to the relevant parties - all automatically within a single, lightning-fast settlement transaction.

Anatomy of a Bet on Zeebit



1. A player selects their bet inputs, sets their stake and hits the button.
2. Within milliseconds, their bet hits a node on the Solana blockchain, which communicates this transaction for processing to all of the validators on the network.
3. The game’s contract will interpret the request, perform validations and convert the bet into a ‘Game Instance’ (for example, schedule that the roulette wheel is to be spun).
4. The player’s bets are each validated with respect to the rules of the game, and if everything’s in order, the Game contract invokes a request to the ‘Cashier’ Contract.
5. The Cashier contract performs some checks based on token balances available - checking minimums and maximums and ensuring both the player and the protocol have the necessary balances to honour their side of the bet, should the bet go in either direction.

6. The Cashier determines the expected edge on the bet, and determines what revenue share needs to take place - between rakeback, bonus pools, referrers/affiliates, platform operators, liquidity providers and the protocol.
7. A request is invoked from the game contract to the verifiable randomness program, which emits events to listening provider nodes. These nodes immediately pick up the transaction emit, take the inputs and produce verifiable randomness which is submitted back to the randomness program.
8. The randomness program checks that everything is in order, and invokes a callback to the game program which uses the randomness to determine the result of the game, and subsequently assesses the result and payouts of the bets.
9. The game contract invokes the Cashier contract, and tells it what funds should be released - either to the liquidity pool in the case of a loss, or paid out directly to the player's wallet, in the case of a win.
10. ...and all of this happens across thousands of validators in just a few milliseconds.

Security Measures

The project intends to undergo full smart contract audits with leading blockchain security firms and publish the results of these audits. Audits will be performed as part of all major releases or upgrades to functionality.

Behind Zeebit

The team behind this project has been developing within the Solana ecosystem space for over two years, and has been behind award winning protocols in Solana hackathons.

The project team is backed by some of the biggest names in Web3 venture capital, including: Jump Crypto, Susquehanna, Mirana, Genesis Block Ventures, PetRock Capital, Blue Pool Capital, Solar Eco Fund, Manna Research, Gate.io, MEXC

Roadmap & Ecosystem Growth

Project Roadmap

In addition to growing Zeebit's range of games, features and token/NFT utility – the roadmap measures below are aimed at removing barriers to adoption and simplifying Web3's existing complexity.

For players who value the principles of decentralization, the platform will always respect and enable full decentralization and transparency in their purest form. Namely full auditability, the ability to interrogate transactions and contracts on block explorers, self-signing, and of course, self-custody and self-management of digital assets.

The Zeebit protocol will always be 100% non-custodial.

Phase I: Platform Launch - Solana & Web3 Early Adopters



Platform & Game Features

The first part of this phase involves launching Zeebit on Solana Mainnet following a condensed Devnet testing phase. On launch, 5-8 original in-house games will be available for players to play.

Community Plans

Early adopters and players are extremely valuable in the early stages of the project, which is why they will accrue early adopter status and become eligible for unique benefits as the project grows.

Broadening Player Activities

A utility centric NFT project will be launched to broaden the number of ways players can interact with the platform at its early stages. The project will also seek to secure key strategic partnerships to bring more value to early players.

Web3 Simplification

From day one, Zeebit's user experience will be superior compared to most decentralized platforms and protocols out there. Early adopters are anticipated to be Solana natives and the Web3 pioneers.

On launch, Zeebit will feature the following features aimed at simplifying and abstracting complexity from today's Web3 user-experience:

- **Sub-second response times** – delivering a lightning-fast experience comparable to response times from a centralized server;
- **Network cost simplification** - the smart contract implicitly covers the network cost of all on-chain state required, removing transaction cost variability. All transactions will incur a fixed, negligible cost of ~\$0.0001 of SOL.
- **Simplified interfaces for managing gas** - enabled by fixed cost gas simplifications above, gas can be measured and presented in a more intuitive way - for example, as 'credits' or based on the number of actions/bets a player can make. (This simplification is a big step from EVM style gas which is variable in three ways: units, unit cost and in the price of the native token.)
- **Instantaneous auto-signing** - Web3auth non-custodial wallet are encouraged on the platform by default - enabling instant, automatic signing and sending of transactions without approvals at every step;
- **Connect with Google, Twitter, Discord, email and more** - Players can choose to access Zeebit without a browser plugin and from any device, sign-up without the need to install anything.
- **Integrated funding and transfer flows** - akin to the user-experience available on Web2 platforms.



Of course, Zeebit is an open and permissionless protocol - the steps taken here are aimed at enabling ease of onboarding and simplified experience by default. For those with a preference for more details, or utilising their own wallets, node providers, token exchanges - these alternatives are available at all times.

Phase II: Broader Web3 Natives - EVM & Cross-chain



Platform & Game Features

In this phase, Zeebit will incrementally add a second wave of games and additional platform features.

Project Token

In the earlier stages of this phase, Zeebits tokenomics will be published and an airdrop eligibility period will begin. Details will be shared and the Zeebit token will be launched and listed on partner exchanges.

Community Plans

Active players and community members will be able to participate in the token airdrop program by engaging in several types of activities related to in-platform and social interactions.

Broadening Player Activities

Today, the majority of Web3 wallet holders and on-chain value exists in the EVM (Ethereum Virtual Machine) ecosystem of blockchains - i.e. on Ethereum and Ethereum side-chains. As of 2022, there are over 30 million MetaMask users globally⁸.

To enable expansion and growth of the community to this next frontier, the following solutions are under development:

- **MetaMask Snaps integration** - MetaMask snaps will enable EVM-natives to easily become Zeebit players, with a wallet abstraction on the Solana blockchain. All controlled securely by their MetaMask wallet, and without the need to install a standalone Solana wallet, to get familiar with Solana conventions or even to use a web3auth wallet.
- **Cross-chain bridging** - Zeebit will leverage Wormhole and a seamless in-app experience to simplify bridging assets to transfer funds to or from Solana. Getting started on Zeebit from supported EVM chains will be as straightforward as funding a Web2 platform, all while retaining self-custody.

Web3 Simplification

Zeebit will continue to simplify and abstract the complexities that come with today's Web3 user experience with the following solutions:

- **Atomic transaction cost rebates** - every transaction will see players rebated the cost of their transaction within the same transaction - effectively creating zero cost interactions. Players will only need to hold only a fraction of SOL in their wallet to interact.
- **Integrated Swaps** - Convenient in-app swapping between tokens supported by the protocol.

⁸ <https://decrypt.co/95039/metamask-consensus-30-million-users>

Phase III: Beyond



Platform & Game Features

In this phase, Zeebit will incrementally launch a third wave of all-original games and platform features.

Broadening Player Activities

Once Zeebit's core platform features are running smoothly, several initiatives will be launched to broaden how players can interact with the ecosystem - namely Token & NFT staking and liquidity provision.

Web3 Simplification

Zeebit's ultimate ambition in this final phase is to provide Web3 novices with a user-experience as simple and familiar as that of the centralized platforms they know and love. The challenge for Web3 developers in working towards mass adoption is to grant everyone the benefits and security that web3 has to offer while removing the hurdles due to complexity.

How this will be achieved:

- **Fully gasless transaction relaying** - Phase 2 atomic gas rebates are a major step, but still require obtaining and holding at least a small amount of native token. With gasless transaction relaying, players can get started with a single currency – just like they would on a Web2 platform. Removing the need to understand concepts like gas, or the need for multiple currencies in parallel is a landmark simplification.
- **Embedded on and off-ramping solutions** -Working with third parties to provide in-app experiences that facilitate on and off-ramping to traditional finance within platform applications.

Partnerships and Composability

As part of Zeebit's growth strategy, the project will seek to onboard and help other protocols to grow through strategic partnerships. Given the core team's technical experience and the composability of the Zeebit protocol, the possibilities are endless.

Some examples of the types of partners Zeebit could work with include:

- **Independent NFT Projects, Communities & Individuals** - Decentralized 'white label' gaming platforms, NFT gated platform benefits, closed competitive leaderboards.
- **Ecosystem Projects** - Integrating third-party project or ecosystem tokens as betting currencies, token gated platform benefits.
- **decentralized Exchanges (DEXs)** - Integrated On-chain Swaps, Atomic Swaps (to support even broader multi-token betting), Token Launches.
- **On-chain NFT Lenders & Marketplaces** - Integrating more features of NFT staking and lending.
- **Infrastructure & Wallet Providers** - Integrating multi-chain infrastructure and unique wallet features such as autosign.
- **DAOs** - Providing exclusive early-stage access to test out new features or games.

