Godzilla Crypto

LitePaper V1.0

ZillaPad is a Web3 multi-chain social task platform incubated by Godzilla Crypto, dedicated to serving more innovative WEB3 projects, assisting them in acquiring high-quality users, and accomplishing initial community launch and virality.

- Users can establish their digital identity and digital asset proof on ZillaPad through Web3 PassPort, earning high-value tokens or NFT incentives for participating in airdrop tasks based on their good digital reputation and behavior on the platform.
- Project owners, on the other hand, can utilize ZillaPad's AirDrop social airdrop task platform, allowing users to earn high-value tokens and NFT incentives through activities like sharing and staking, thus gaining more users and building a stronger product and community.

The Composition of the Godzilla Crypto ZillaPad Project

- Web3 PassPort, Identity and Behavior, Asset Digitization
- AirDrop Airdrop Task Platform
  - Composable Airdrop Task Platform
  - AI-Based Big Data Analysis, Anti-Sybil Algorithm
- DAO Community Governance, Revenue Sharing

1. Goals and Vision

In the future Web3 world, Godzilla Crypto envisions a scenario where everyone can earn cryptocurrency and valuable NFTs through Web3 PassPort and AirDrop airdrop tasks. The time and effort users invest can be quantified digitally, ensuring a tangible return. Concurrently, Godzilla Crypto's Web3 PassPort digital identity system aims to assist project owners in acquiring a genuine and reliable user base, mitigating losses caused by Sybil attacks.

- AirDrop Social Task Traffic Entry

Godzilla comes with SocialFI social features, allowing project owners to use ZillaPad Space's task platform to release information and create a community entry point. Various airdrop tasks can be published to drive community engagement.

- Web3 PassPort Digital Identity, Asset Self-Sovereignty, Privacy Protection

Decentralized mechanisms rely on a 'unique identity assumption' – each participant in the network has an independent identity, with equal voices among different identities. Godzilla, through collaboration with oracle platforms like Chainlink, can achieve on-chain representation of user offline identities (such as ID, Twitter, Telegram) and behavioral information (like sharing, following, liking) through zero-knowledge verification, associating them with their digital identity. This forms a comprehensive Web3 on-chain digital identity system. Within this system, users can establish not only their ID but also a digital reputation and asset certification formed through accumulated behavior. Project owners can create sharing tasks based on the user's digital identity system, granting tokens or NFTs based on user behavior, fostering community expansion.

Since Web3 Passport is established on-chain, it avoids the risks of information leakage and sale that come with centralized management of user information by operators in the traditional Web2 era, achieving user digital identity self-sovereignty and privacy protection.

- AI Algorithms, Sybil Attack Defense

On the Godzilla Crypto platform, users, while completing airdrop tasks and receiving rewards, actively transform into a project's community,

enabling a secondary spread for the project and achieving a win-win situation for both the project owner and users. Simultaneously, ZillaPad's Web3 Passport and backend AI algorithms filter out Sybil attacks, preventing the theft of assets from project owners.

- DAO Community Governance

Godzilla Crypto employs a DAO decentralized community governance structure. Users holding GODZ tokens can participate in community proposals and voting. Godzilla Crypto's DAO includes features like investment management treasury, community incentive activities treasury, and wallet management. It manages the value generated through fundraising or operational activities. Additionally, holding GODZ allows participation in Godzilla Crypto ZillaPad's token airdrops, staking incentives, Web3 Passport level forging, and other activities, offering high-value incentives in return for holding GODZ.

2. Web3 PassPort

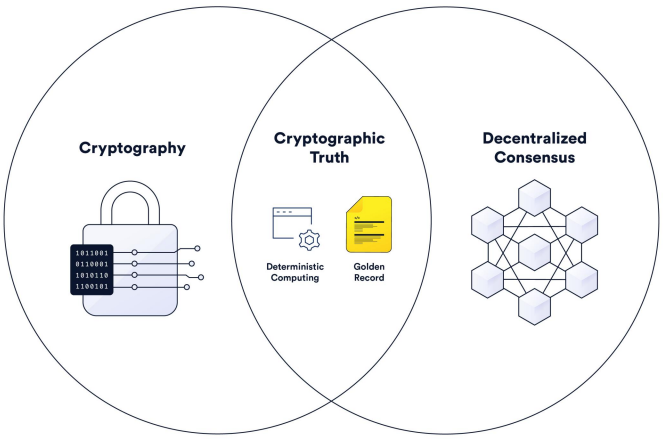
1) Web3 Digital Identity Background

Web3 has brought numerous benefits to society, lowering capital barriers, enhancing application transparency and encryption security, and providing decentralized financial services to the public. Despite the significant success of Web3, it faces the risk of hyper-financialization. If hyper-financialization occurs, individuals with the most financial resources will have excessive influence over core areas such as ecosystem development, governance, and culture. Currently, Web3 users know little about each other beyond their on-chain addresses. To unlock more innovative application scenarios, Web3 needs to establish a

technical stack based on users' economic and social attributes. This way, on-chain relationships can extend beyond transactions to include personal connections, culture, reputation, identity, and trust across various dimensions.

2) Why Web3 PassPort is Needed

The core of Web3 is to achieve trust minimization, ensuring that processes unfold almost exactly as participants anticipate. Blockchain employs decentralization, economic incentives, and encryption technologies to achieve trust minimization, safeguarding users against inaccuracies, timeliness issues, susceptibility to manipulation, and tampering. Executing code and storing data on the blockchain in a trust-minimized manner is often referred to as 'cryptographic truth.



However, the current challenge is that relying solely on economic incentives is insufficient to build a framework for end-users to engage in social and economic activities. Firstly, in certain application scenarios, the penalty mechanisms established to achieve trust minimization may be too stringent, with punishments outweighing rewards. In such cases, users may find it impractical, especially if fines result from accidents or misunderstandings. In many application scenarios, users prefer not to be impacted by economic factors, or at least, they do not want to undertake

risks, such as staking significant assets in interactions, particularly in governance, public goods, and social clubs.

Therefore, there is an urgent need to create an on-chain identity layer for Web3. This layer should prove users' social identities to blockchain applications while safeguarding their reputation, KYC/AML, personalized data privacy, and, to some extent, or entirely, retaining the characteristics of trust minimization on the blockchain. Identity solutions can assist users and applications in understanding information beyond user account balances and transaction histories. They can facilitate on-chain interactions based on various types of social information.

This is the reason behind the creation of Godzilla Crypto Web3 PassPort. With an increasing user base, Godzilla Crypto Web3 PassPort will also be open to more Web3 application developers, forming a vast ecosystem of applications and enabling the on-chain roaming of user digital assets.

3) Web3 PassPort Solutions

Godzilla Crypto's identity solution for Web3 is primarily divided into three main categories. These can be used individually or combined to meet various needs.

- Blockchain: Identity Database

Blockchain serves as a public database, and technically, the data stored by users cannot be tampered with. Anyone worldwide can access this data, making it easily applicable to various scenarios. However, storing raw personal identity information (PII) on public chains may lead to serious privacy issues due to the inherently transparent nature of

public chains. There are alternative methods to access blockchain identity data and assertions:

- Users can store the hash value of personal identity information data on the blockchain, while the data itself is stored in an off-chain database;
- Personal identity information or claims about data can be transformed into tokens on the blockchain;
- External entities (i.e., blockchain) can be used to verify a user's off-chain identity information, and the proof can be published on-chain for smart contracts to reference (e.g., publishing a proof, a 'yes' or 'no,' demonstrating whether Alice is over 21).

- Identity Proof: Identity Information and Attestation

Identity proof refers to claims about an individual's qualifications, achievements, characteristics, or any background information. Identity solutions use proof to verify whether an individual is eligible to perform certain operations. For example, only individuals with a driver's license can drive a car, or those with relevant professional certifications can practice in a particular industry.

The fundamental purpose of Web3 is to establish digital relationships. To develop Web3 identity solutions, the key is to access verifiable proofs. Two common features of Web3 identity are verifiable credentials and decentralized identity (DID). Verifiable credentials are immutable statements about a user's identity, cryptographically signed by the issuer. Verifiers can use DIDs to verify these identity proofs, utilizing public-private key pairs on the blockchain to verify hashed identity proofs belonging to a specific user.

Additionally, identity data or proofs can be tokenized. For instance, Soul-Bound Tokens (SBT) are non-transferable non-fungible tokens (NFTs) representing commitments, qualifications, membership,

affiliations, or statements of token owners. SBTs can be issued by users to other users or by institutions, including various information such as university-issued degree certificates or statements users wish to be publicly accountable for. While SBTs provide a reliable unique identity for on-chain addresses, they are inherently transparent, making them less suitable for privacy-centric scenarios. Proof-of-Attendance Tokens (POAPs) are another tokenized identity solution where event organizers issue NFTs to participants, proving their involvement in an event.

Users can combine tokenized and non-tokenized identity proofs, having the authority to control both types of identity proofs. This lays the foundation for decentralized identity or self-sovereign identity (SSI). The essence of this concept is that users can own and manage their identity proofs, sharing them with applications as desired.

- Oracle: Validators and Transmitters of Identity Proof

Oracles can verify and upload user identity information originally stored off-chain or generated off-chain to the blockchain. Oracles can directly transmit raw data from off-chain APIs to the chain or transfer data between different blockchains. Before uploading data to the chain and triggering on-chain executions (e.g., minting tokens based on some off-chain personal identity data), oracles can perform computations on the raw data.

A novel application of oracles allows users to request their own data, such as obtaining a degree certificate from a university or legal proof from a government website. Users do not need to expose data privacy to oracles; they can prove their data through zero-knowledge assertions. Ultimately, oracles can verify the validity of users' off-chain identity information while safeguarding data privacy.

Godzilla Crypto achieves the transfer of off-chain information to the chain with the collaboration of well-known oracle platforms such as Chainlink.

4 Airdrop Task Platform

Godzilla Crypto is set to create an open airdrop task service platform called ZillaPad Airdrop. Through the ZillaPad Airdrop Task Management platform, users can explore and learn about various projects. They can earn corresponding rewards by completing airdrop tasks, such as NFTs, POAPs, airdrop eligibility, token rewards, etc. Zero investment, zero risk.

ZillaPad Airdrop Task Management platform aims to become the foundational platform for on-chain credentials in the Web3 world. Collaborating project partners can independently launch project spaces on the ZillaPad Airdrop Task Management platform and initiate airdrop tasks. Once users connect their wallets and log in, they can view ongoing task activities on ZillaPad Airdrop, with detailed descriptions including event introductions, duration, and qualification criteria for earning rewards.

By integrating with WEB3 PassPort and decentralized autonomous organization (DAO), ZillaPad Airdrop transparently and in a decentralized manner manages tasks and rewards. It assists in onboarding new members and serves as the primary gateway for project community traffic.

5 AI Analysis & Anti-Sybil Algorithm

1) Airdrops and Freeloaders

From September 2020, when Uniswap initiated the airdrop frenzy, to the present, which is less than three years, airdrops have undergone significant changes in form, nature, and participation scale. Airdrops are no longer just on-chain celebrations; various stakeholders, including liquidity providers, centralized exchanges, and wallets, have become involved. Consequently, scenes such as exchange rushes, whale dumping, gas wars, and project website crashes have started to occur frequently.

However, both project teams and freeloaders continue to escalate their tactics in this cat-and-mouse game, gradually evolving into a peculiar relationship of mutual antagonism and interdependence.

2) Sybil Attack

Sybil attacks in the Web3 world compromise the fairness of airdrops. Speculators unfairly acquire more airdrop tokens by creating false accounts. Such attacks often occur when a user employs multiple fake identities (resembling a witch with multiple identities) to disrupt or gain control of the network in various ways. In recent years, there has been an increasing prevalence of online false identities and distributed denial-of-service (DDoS) attacks in the blockchain domain.

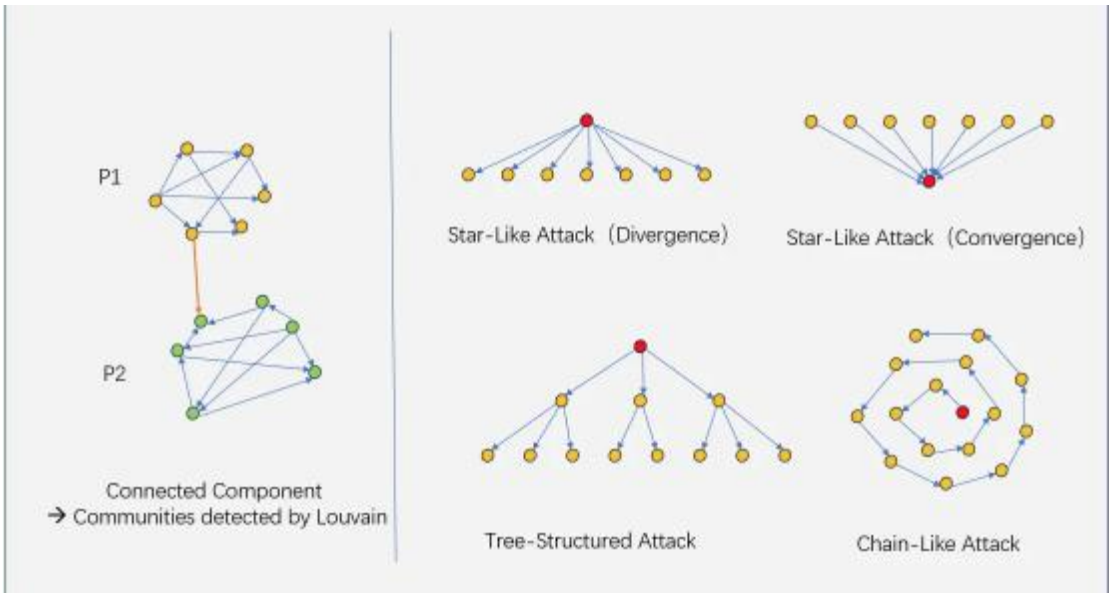
3) Godzilla AI Countering Sybil Attacks

Witches use bots and automated scripts to interact with their accounts and the blockchain. These accounts, due to their interconnections and similar behaviors, should logically be clustered into malicious groups. Godzilla, through technical collaboration with strategic partners, has designed a two-stage framework to identify witch groups using AI-ML clustering algorithms:

- **Stage One**

Utilize community detection algorithms like Louvain and K-CORE to analyze asset transfer graphs (ATGs) and detect closely connected and suspicious witch groups.

Godzilla analyzes the following ATGs to detect witch groups.



- As shown in the diagram, ATGs are decomposed into connected graphs like P1+P2. Community detection algorithms (such as Louvain) break down larger connected graphs into more densely connected groups to optimize the modularity metric, as seen in subgroups like P1 and P2, which can be obtained by cutting fewer edges.
- As illustrated, Godzilla identifies witch groups based on known attack

patterns.

- Starburst Dispersal Attack: Addresses within the group receive transfers from the same source address.
- Starburst Convergence Attack: Addresses within the group send funds to the same target address.
- Tree-like Attack: Fund transfer relationships within the group form a tree-like topology.
- Chain-like Attack: Sequential transfers between addresses form a chain-like structure.

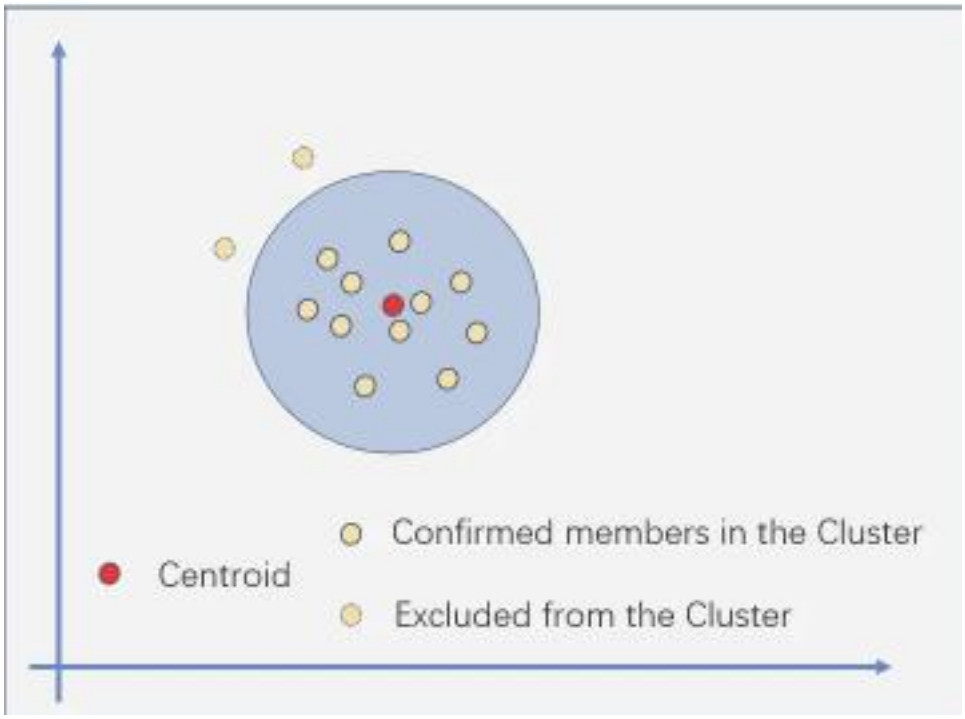
- Stage Two

Analyze the user profiles and on-chain behaviors of each address. Godzilla uses the K-means algorithm to further filter similar addresses and optimize the clustering results obtained in Phase One, reducing false positives.

Godzilla initially employs graph mining algorithms to identify witch groups and then enhances accuracy by filtering out misidentified addresses through user behavior analysis. By combining user association analysis with behavior analysis, Godzilla's witch detection solution becomes more reliable and stable.

Transaction records reveal address behavior patterns. Witch accounts within a group may exhibit similarities in interacting with the same contracts/functions, as well as similarities in interaction time and amounts. Godzilla optimizes Phase One's groupings by analyzing two types of on-chain behavior variables:

- ransaction Variables: These variables directly derive from on-chain operational behavior, such as the first and latest transaction dates and information about the protocols or smart contracts involved.
- Profile Variables: These variables provide aggregated statistical data on address-related behavior, including interaction count, frequency, and quantity.



Based on the multi-dimensional data representation of address behavior, Godzilla utilizes a K-means-like algorithm process to optimize the witch groups identified in Phase One.

As shown in the diagram above, the calculation process is as follows:

- Step 1: Compute the centroids of the groups:

For continuous variables, calculate the mean for all addresses within each group.

For categorical variables, determine the mode for all addresses within each group.

- Step 2: Optimize the groups by excluding addresses far from the centroids using a predefined threshold:

Addresses that are too far from the centroids are excluded from the groups.

Update group membership based on the refined address set.

Iterate through these two steps until convergence is reached, resulting in optimized witch groups.

6 Godzilla Crypto DAO

In the Godzilla Crypto DAO, two community-managed cryptocurrency wallets have been established for the public. These wallets are designated for the management of value currencies, including but not limited to GODZ, USDT, BNB, ETH, and are utilized for community participation in the DAO and the management of community incentive activities.

Marketing.zillapad

0x8Bd01C1BEC261B8d802208ca85948248822a3E8c

Foundation.zillapad

0xE22ABaF38eda971e0A4b0aeA0B2108cec1B8296a

As of December 23, 2023, the DAO fund has successfully raised 24 trillion GODZ tokens, which are currently allocated for community incentive activities, including airdrops. The upcoming launch of the third round of fundraising involving USDT/BNB will be directed towards the subsequent management of the GODZ/BNB liquidity pool.

Furthermore, Godzilla Crypto ZillaPad is gearing up to introduce staking opportunities for GODZ, allowing community users to earn project token airdrops, NFT airdrops, and inscription airdrops. This initiative aims to provide GODZ holders with additional opportunities to receive high-value tokens and NFTs, beyond the contractual trading dividends associated with GODZ.

The DAO's proposal and voting platform are scheduled to go live in the second quarter of 2024. For more detailed information, please refer to the DAO description on blog.zillapad.com.

7 RoadMap

2021-08-06	GODZ Contract Fair Launched
2023-12-23	Publication of Godzilla Crypto LitePaper v1.1.2
2024-Q1	Launch of Godzilla Crypto ZillaPad AirDrop
2024-Q2	Alpha Testing of Godzilla Crypto Web3 PassPort
2024-Q3	Release of Godzilla Crypto Web3 PassPort