



# **BUILDING TRUST IN THE CRYPTO ECOSYSTEM**

*A Policy Paper by Binance*

# INTRODUCTION

Blockchain is one of the most fascinating innovations of our generation, revolutionizing numerous products and services within financial services and beyond. Cryptocurrencies, perhaps the most recognizable application of distributed ledger technology, have thorough and sophisticated technological underpinnings, innovative applications and untapped potential and utility - all making them incredibly viable and valuable as both technology and business endeavors.

2022 was an historic year for the crypto industry. This was a watershed moment where rebuilding user and regulator trust is critical for the future of the whole ecosystem. Users will demand more from centralized exchanges, and the exchanges must rise to the occasion.

With this in mind, all players in the digital assets space have a fundamental responsibility and part to play to prove that a few bad actors are not emblematic of the industry. Winning back policymakers, regulators, and the community's trust will require putting risk management, security, and transparency front and center.



“Everybody in the industry has the responsibility to protect users. We hope industry players can cooperate to gather opinions and set strong standards. Given the recent series of events in this year, Binance sees the importance of developing common guidelines. We will try to get together with other industry players to form common business standards. All industry players need to increase transparency and work closely with regulators to make the industry more robust.”

*CZ at the B20 conference in Bali, Indonesia, November 2022.*

## EXECUTIVE SUMMARY

This paper proposes a detailed, actionable framework of guidelines for all centralized exchanges (CEXs) to raise the bar on trust and safety across the industry.

It also shares Binance's efforts to uphold those commitments. We propose these guidelines from a place of humility and duty towards the community, and continue to iterate and improve.

# PROPOSED INDUSTRY GUIDELINES

## Handling Customer Assets

### **Prevent Unauthorized Use of Customer Assets**

Exchanges must be risk averse with user funds. Customer assets should never be used in any other way than what the customer consents to under the terms of specific products.

### **Wallet Infrastructure and Security**

Centralized exchanges must allow users the freedom to choose where to store their digital assets, depending on their unique needs, trading habits and independent risk evaluation of the various solutions available. Depositing and withdrawing crypto assets into/from the exchange for the purpose of trading should be a simple, cost-efficient and seamless process.

Centralized exchanges must adopt the highest security standard solutions for the storage of customer assets to protect them from cyber threats.

## Transparency and Disclosures

### **CEX Operations must be Transparent**

Users have the right to verify the safekeeping of their assets held in a CEX's custody, through proof of reserves or similar disclosures.

### **Disclosure Method and Process**

The disclosure method used must be technically adequate, updated on a regular basis and based on reliable technology that cannot be falsified (such as zk-SNARKs).

## Risk Management

### **Conservative Capital Structures**

Efficient use of capital is critical for CEXs. The risks of using debt to fund growth are exacerbated by crypto's volatility, and companies are urged to maintain a conservative capital structure.

### **Properly Collateralized Wrapped Tokens**

Wrapped tokens offered by a CEX for use on a different blockchain must always be collateralized 1:1 on their native blockchain.

The collateral reserves must be publicly visible to and verifiable by the community.

### **Token Listing Governance**

CEXs have a critical responsibility to implement a strict governance process for admitting crypto assets to trading on their platforms to protect users from low credibility projects with little or no utility.

### **User Protection Funds**

Centralized Exchanges should establish a reserve to act as a safety net in situations such as a security breach.

### **Education**

All exchanges must dedicate significant resources to provide their users with sufficient knowledge about their products, services and the broader industry.

Materials should clearly explain the risks associated to enable users to make informed choices.

### **Loans Must be Appropriately Collateralized**

CEXs that offer loan or margin/leveraged products should ensure that these are appropriately collateralized.



# HANDLING CUSTOMER ASSETS

Customer assets should be safely stored and protected, and ***never used in any other way than what the customer consents to.***

## BEST PRACTICES

***What every CEX must do***

### **1- Prevent Unauthorized Use of Customer Assets**

Customer funds should never be used in any manner or for any other purpose than what the customer consents to under the terms of specific products.

### **2- Wallet Infrastructure and Security**

CEXs must provide users with clear information on their options for storing their digital assets, and the freedom to choose the solution that works best for their unique needs, trading habits, and independent risk evaluation.

Depositing and withdrawing crypto assets into/from the exchange for the purpose of trading should be a simple, cost-efficient, and seamless process, regardless of the user's choice of safekeeping solution.

Exchanges must adopt the highest security standards for assets held in their custody to minimize risk to user funds.

## BINANCE

***How Binance is working to meet those standards***

At Binance, our role, first and foremost, is to protect our users.

### **1- Use of Customer Assets**

Binance holds user assets 1:1, protected by the highest wallet security standards, and does not use them to deal on its own account or for any other purpose without customer consent under the terms of specific products.

## 2- Wallet Infrastructure and Security

Binance uses its own wallet infrastructure to safeguard user assets and its proprietary assets.

As one of the largest custodians of assets in the crypto space, security is at the top of our priority list. In order to enable this, we spend hundreds of millions of dollars on security, hiring the best people and employing the best technology. It is one of the single largest investments that we make each year. You can read more about how cryptography is used for wallet security in this [paper by Binance Research](#).

We believe that our wallet infrastructure is one of the most secure in the industry. We have considered the use of third party wallet software. However, we have reviewed other wallet vendors and are much more confident in the security of our own ecosystem than what we have seen from other vendors.

Additionally, we have been continuously working to improve Trust Wallet, a self-custodial and multi-chain wallet service provider - and part of the broader Binance ecosystem. Last November, Trust Wallet [rolled out a new browser extension](#) crypto wallet and [Binance Pay integration](#) to grant users straightforward access and provide them with another option for the safekeeping of their assets (self-custody).

# TRANSPARENCY AND DISCLOSURES

Exchange operations must be transparent. Users have the right to **verify the safekeeping of their assets** held in a centralized exchange's custody.

## BEST PRACTICES

### *What every CEX must do*

Properly conducting proof of custody reserves is a very complex process which is new and unique to the industry, and is rather different from traditional financial institutions.

Luckily, technology has made innovative solutions possible. Below are some guidelines on how the desired transparency can be achieved for CEX users to ensure their assets are collateralized, exist on the blockchain and are under the control of the exchange at the reporting date.

### **Disclosure Method: Merkle Tree with zk-SNARKs**

CEXs should publish a proof of reserves tool based on Merkle tree and zk-SNARKs technologies.

Combining zk-SNARKs and Merkle tree proof gives users a new and improved way of verifying the safekeeping of their assets. Specifically, using zk-SNARKs allows users to check that each account's total net balance is non-negative and that all user assets are part of a CEX's claimed total net balance of user assets – in a private and secure manner.

zk-SNARKs provide the technology needed to ensure both data integrity and privacy at the same time. Its application for proving reserves and increasing CEX transparency should help build trust in the blockchain industry. For many, a development like this has been long awaited and comes at a pivotal time for CEXs.

## More About the Technology

### Classic Merkle Tree

A Merkle Tree is a cryptographic tool that consolidates large amounts of data into a single hash value. The hash value - known as a “Merkle Root” - acts as a cryptographic seal that essentially summarizes all the inputted data. Merkle Trees are used by centralized exchanges for their PoR assessments to verify that individual user accounts are included within the liabilities report to be inspected by auditors.

Merkle Trees make a great tool for the purpose of verifying an exchange’s holdings for the following reasons:

- **Anonymity:** Merkle Trees can confirm the safekeeping of the assets in question, without revealing individual user balances
- **Verifiability:** They give users the ability to independently verify their individual funds were included within the assessment
- **Tamper-Proofing:** Any change to the data alters the Merkle Root i.e. the unifying signature or all assets under the tree.

### How It Works

The classic Merkle tree entails inserting the customer balance table into a Merkle sum tree. Each node in a Merkle sum tree is a (balance, hash) pair. The bottom-layer leaf nodes represent individual customers’ balances and salted username hashes. The balance in each higher-layer node is the sum of the two balances below it, and the hash is the hash of the two nodes below it. A Merkle sum proof, like a Merkle proof, is a “branch” of the tree made up of the sister nodes that run from a leaf to the root.

## zk-SNARKs Technology for Proof of Reserves

zk-SNARKs can be a powerful tool that brings additional privacy and simplicity benefits to proof of reserves and liabilities. The idea was initially proposed in this [blog post](#) by Vitalik in November 2022, and in February 2023, Binance implemented the first real life solution utilizing this technology for proof of reserves. For more details on Binance's solution, see [this link](#).

### About Zero Knowledge Proof and zk-SNARKs

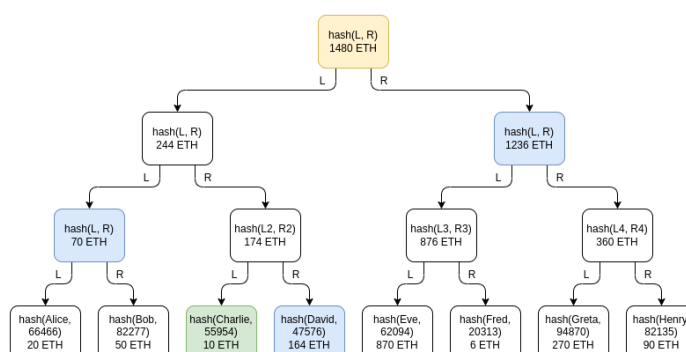
zk-SNARKs (Zero-Knowledge, Succinct, Non-Interactive Arguments of Knowledge) are a form of cryptographic proof that allow one party, the prover, to demonstrate to another party, the verifier, that the prover had executed certain computations accurately with certain inputs under certain constraints, all without disclosing the inputs.

The computation might be time-consuming, but the underlying mathematical mechanism can help the verifier assess the proof quickly and securely. To take a deeper look under zk-SNARKs' hood, you can refer to this [series of articles](#).

### What zk-SNARKs can deliver

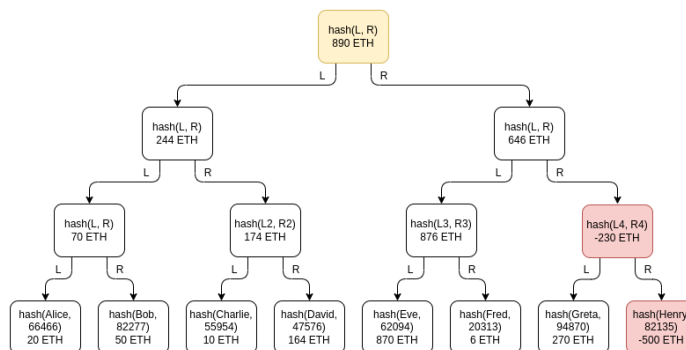
zk-SNARKs can address the 2 key limitations of a classic Merkle tree (see the diagrams for more detail):

1- You can prove that user balances add up to the claimed total without revealing information about other user balances:



*e.g. Charlie's proof would include all the information in the blue nodes. He will know that a user has 164 ETH, two users have balances adding up to 70 ETH ...etc. Even if anonymized, bad actors can utilize this information maliciously. (Source: [vitalik.ca](#))*

2- The CEX could potentially add a negative balance under a fake account somewhere in the tree to make the total required reserves appear smaller.



Source: [vitalik.ca](https://vitalik.ca)

The new solution combining both Merkle tree and zk-SNARKs proves that:

1. All leaf nodes of the Merkle tree have contributed to Binance's claimed total user balance of each asset.
2. There is no user with a negative total net balance (an overall USD value of all assets the user holds) included in the Merkle tree.

## BINANCE

*How Binance is  
working to meet those  
standards*

Binance is in the process of making continuous and significant enhancements to its PoR system. We started by disclosing our hot and cold [wallet addresses](#), and followed with our [Merkle tree proof of reserves tool](#) in November 2022.

In February 2023, we upgraded our PoR system with zk-SNARK, a zero-knowledge verification method that helps to keep your sensitive information even more private and secure and would require an unfeasible amount of computational power to break its security.

This is the first version of our zk-SNARKs implementation and we are looking forward to receiving [community feedback](#) so we can continue to improve the system.

For More Information:

- [What Is Proof of Reserves](#)
- [How zk-SNARKs Improve Binance's Proof of Reserves System](#)
- [What Is Merkle Tree](#)
- [Improving Crypto Transparency With Zero-Knowledge Proof](#)

With our latest update, 80% of our assets are covered, and we will continue to add more tokens and work to make the verification function more reliable, secure and private.

We have also made our code for Binance's PoR system **open-source** to provide even more transparency for our users and so that others in our industry and community can benefit from this important technology. We encourage all CEXs to make use of this solution, and the whole community to share feedback so we continue to improve it further.

# RISK MANAGEMENT

User funds must never be mismanaged. Centralized exchanges must adopt **strict risk management measures** to protect users and their assets.

## BEST PRACTICES

*What every CEX must do*

### 1- Conservative Capital Structures

**Taking on debt to fund growth should be approached with caution**

With the past year's macroeconomic and geopolitical developments, it has become clear that efficient use of capital is critical to any company's success. Even more established, less volatile sectors than crypto are pivoting towards a more conservative stance on taking on leverage to fund growth.

The risks are exacerbated by the volatile nature of the crypto assets industry. Companies in the cryptocurrency and digital assets space are urged to maintain a conservative approach to their capital structure. The perpetual fluctuation in value of cryptocurrencies, especially in its nascent days, makes it extra challenging and generally inadvisable to rely on debt to fund growth.

### 2- Properly Collateralized Wrapped Tokens

**Wrapped tokens must always be collateralized 1:1 on their native chain**

Wrapped tokens offer a great interoperability solution allowing users to seamlessly move assets and make use of applications, projects, and opportunities on other blockchains.

This brings various benefits such as faster transaction times, lower gas and other fees, yield farming opportunities, and other use cases.

To ensure value stability, wrapped tokens must always be collateralized 1:1 on their native chain, with the collateral clearly set aside in a manner verifiable by the community.



### 3- Token Listing Requirements

#### Maintain high standards for admission of assets into trading

Centralized exchanges have a critical responsibility to implement a strict governance process for admitting crypto assets to trading on their platforms. A stringent due diligence process and strict listing requirements must be self-imposed by all centralized exchanges to protect their users from projects with low credibility and high risk.

### 4- User Protection Funds

#### Additional safety nets in case things go wrong

**User Protection Funds:** Exchanges should establish a reserve to act as a safety net to protect users in the event of data security threats.

Some best practices:

- A periodic review of the fund's total value must be conducted, and top-ups might be necessary to maintain a reasonable level of coverage during market downturns.
- The fund assets must be safekept such that they are not compromised in the same manner in the unfortunate event that the CEX's funds were subject to a security breach.

#### **Industry Recovery Funds:**

CEX's should consider participating in industry wide efforts to support high potential projects in the digital assets and Web3 space that could be facing funding difficulties during broader market downturns.

### 5- Education

Education is the best form of consumer protection. Spreading financial literacy for crypto assets and making blockchain education accessible is key to mass adoption.

All exchanges must dedicate the necessary resources to provide their users with sufficient knowledge about their products and services to choose the products, services, and vendors that cater to their needs. Providing the right level of knowledge and investing in user education is pivotal to the future of the whole industry.

## **BINANCE**

*How Binance is  
working to meet those  
standards*

### **6- Loans Must be Appropriately Collateralized**

CEXs that offer loan or margin/leveraged products should ensure that these are appropriately collateralized.

#### **1- Conservative Capital Structure**

At Binance, we believe that it is unwise to take on debt to fund growth which is why Binance's capital structure is debt free.

#### **2- Properly Collateralized Wrapped Tokens**

Binance provides users with a few options for wrapped tokens to use on different chains, such as BTCB and BBTC.

Our wrapped tokens are always collateralized 1:1, and the community can verify this here: <https://www.binance.com/en/collateral-btokens>.

We also conduct periodic burns of the wrapped tokens to ensure their stability of value in case demand fluctuates.

#### **3- Token Listing Requirements**

Binance has a very strict listing process to admit tokens for trading on its platform.

To illustrate the robustness of our listing procedure, for Binance Launchpad and Launchpool, out of 450 applications in the first half of 2022, only 5 projects were listed. The statistics are similar for direct listings, where only around 1% of tokens are successfully listed on the Binance platform. You can learn more about listing coins on Binance [here](#).

#### **4- User Protection Funds**

##### **1- SAFU**

On Nov 9, 2022, Binance announced it has topped up its Secure Asset Fund for Users (SAFU) to \$1B in order to continue to provide industry-leading protection to users.

- Binance has pledged to monitor the SAFU on an ongoing basis to ensure its size remains adequate to protect users' interests. Users can view the wallet addresses where the funds are stored [here](#) and [here](#).

- Today, there is about 1 billion USD in the fund. We are encouraging other industry players to implement a similar user fund protection mechanism.

## 2- Industry Recovery Initiative (IRI)

A co-investment opportunity for organizations eager to support the future of Web3. You can learn more about this initiative [here](#).

## 3- Insurance Funds

Other safety features such as insurance funds for our Futures product protect users from adverse losses. Insurance funds protect bankrupt traders from adverse losses and ensure that the profits of winning traders are paid out in full. The primary purpose of an insurance fund is to limit the occurrences of auto-deleverage liquidations (ADLs). Due to the volatility in the crypto markets, and the leverage offered to clients, it is not possible to fully avoid auto-deleverage liquidations. In order to provide the best possible client experience, we strive to keep auto-deleverage liquidations to an absolute minimum.

## 5- Education

### Binance Academy

Binance Academy is an open access blockchain and crypto learning portal that hosts free educational resources in over 25 languages, including 386+ articles in addition to videos, and online courses on a variety of topics such as: blockchain, cryptocurrency, security, technology, and more. For more information, visit <https://academy.binance.com/en>.

In November 2022, Binance Academy launched the first online course series, with more added regularly <https://academy.binance.com/en/courses>.

The content has been useful for governments, regulators and the global crypto community. The Portuguese government, in fact, uses Binance Academy content on their government website.

All content on Binance Academy is completely free. With no

advertisements, no requirement for payment or registration, everyone can learn at their own pace and even earn free crypto through learning by taking part in the [Learn and Earn](#) program.

### Responsible Trading Program

Binance was the first digital assets exchange to launch a [responsible trading program](#) for derivatives and the first major crypto exchange to create more [stringent guidelines surrounding leveraged products](#).

### Other Educational Programs and Resources

- **Binance Masterclass:** an in-classroom educational program. We have educated more than 600k people in the past 4 years.
- **Binance Scholarship:** Binance supports full scholarships including blockchain certifications. We currently work with a dozen universities in France, Italy and Spain, and are talking to a lot more.
- **Law Enforcement Education Program:** this team set up educational seminars for law enforcement agencies all around the world, including France, Dubai, Canada, Brazil, and many more.
- Other educational initiatives of Binance Academy include the University Outreach Program across 15+ countries, [Student Ambassador Program](#), partnerships with top online learning platforms, professional associations, industry alliances, and others.

## 6- Loans Must be Appropriately Collateralized

Binance's loan and margin products are always fully collateralized. You can learn more [here](#).

# GLOSSARY OF TRANSPARENCY AND TRUST TERMS

This glossary unpacks various frequently used terms, tools and methods that have been used by the industry to address trust issues.

## Transparency

### **Proof of Reserves**

In the context of centralized cryptocurrency exchanges: a statement, tool, or report showing that assets held by the exchange are equal to or greater than their liabilities to their customers.

### **Safekeeping of User Assets**

A financial services provider, broker, or other custodian, storing an asset on behalf of their customers. The custodian is responsible for the safekeeping of the assets and implementing the necessary security standards, without expectation or authorization to use the assets in any other manner without customer consent.

### **Merkle Tree**

A cryptographic tool that consolidates large amounts of data into a single hash value. It is named after Ralph Merkle, who patented it in 1979. Merkle trees can verify that information blocks belonging to a given dataset have been undamaged and unaltered.

Merkle trees can be used as a tool to verify user balances held on a centralized cryptocurrency exchange by providing an anonymized, independently verifiable snapshot of all user balances at a given point in time.

### **Merkle Sum Tree**

A Merkle Sum Tree is a type of Merkle tree that verifies there is no change in the cumulative value or distribution of the

‘leaves’ of the tree - i.e. the blocks of information contained under it.

### **Merkle Tree Root**

The shared hash value of all nodes in a Merkle tree that acts as a cryptographic seal - essentially summarizing all the inputted data belonging to the tree. Any tampering with the data affects the Merkle root, making it obvious and easy to spot.

### **Merkle Tree Leaf**

A block of information contained under a Merkle Tree. In a PoR Merkle Tree, the leaves contain information about an individual user’s balance and account information that is cryptographically stored.

### **zk-SNARKS**

Zero knowledge succinct non-interactive argument of knowledge: a cryptographic proof of knowledge method whereby one party (the prover) can show evidence to the other party (the verifier) that they possess a certain piece of information, without the verifier needing to have that information or interact with it.

## **Risk Management**

---

### **Wrapped Tokens**

A cryptographic token issued in parallel to a particular cryptocurrency (or other digital asset), that allows users to utilize the aforementioned cryptocurrency on a different ecosystem other than its native blockchain.

The wrapped token issuer sets aside an amount of the cryptocurrency as collateral, stores it safely, and then “mints” the wrapped token at a 1:1 ratio based on the collateral. Wrapped tokens thus offer a great interoperability solution allowing users to seamlessly move assets and make use of applications, projects, and opportunities on other blockchains.

**Auto liquidation**

A risk mitigation measure in crypto margin trading. When the price of the crypto asset being traded falls below a certain threshold(s), a trader's leveraged position is forced to partially or fully close, due to the margin not being enough to cover the loss. If the trader is unable to meet the margin call, the exchange closes the position automatically.

**SAFU**

An emergency user protection reserve which offers protection to Binance users in the event of a security breach.

**Responsible Trading Program**

A set of policies and materials aiming to discourage and prevent risky behavior among users of a trading market for high-risk or volatile instruments, such as derivatives. You can see Binance's responsible trading program [here](#).