CEFFU

Our approach to institutional custody to secure client assets

2023 Security Report

Your secure gateway to an institutional ecosystem built to keep your assets safe

Since launching its institutional services in December 2021, Ceffu has devoted its operational and technological resources to growing a compliant, audited, institutional-grade infrastructure that addresses the ever-growing needs of global clients, the likes of large financial services firms, institutional investors, and crypto-native firms. Within just over a year of operation, we have set and achieved numerous milestones to create a safe environment that supports the adoption and participation of institutions in the digital asset economy by enabling them to secure, manage, and utilize their assets efficiently while ensuring the utmost security measures are in place.

Ceffu is registered as a Virtual Asset Service Provider (VASP) with the local Financial Intelligence Unit in Lithuania, subject to regulatory oversight. Our platform and services are operated by a dedicated team of experts from traditional finance, cryptocurrency exchanges, blockchain and customer asset security, working together to ensure the necessary governance controls and security measures are implemented to safeguard our clients and their digital assets.

Committed to best-in-class security and privacy protection

As a compliant institutional custodian, our priority is to grow a safe and reliable platform that institutional clients can entrust with the security of their assets, as well as their data. Receiving our ISO 27001 & 27701 certifications by the British Standards Institution (BSI), as well as our SOC 2 Type 1 & Type 2 attestations from Armanino LLP, affirms this priority as we continue to provide and maintain the highest level of security and operational compliance. Ceffu is built on a legacy of user-centric values that have helped us develop an entire suite of integrated, institutional-grade custody solutions that not only address the ever-growing needs of institutions but also meet regulatory and compliance requirements.

As we continue to provide and maintain such robust levels of security and risk management, our platform also undergoes penetration tests performed by an independent third-party security firm. These tests simulate authorized cyberattacks against computer systems to evaluate our security architecture. Other security exercises, including phishing tests, are also conducted periodically to ensure our systems are highly protected.

ISO 27001

ISO 27701

SOC 2 Type 1 & Type 2

Our security pillars

Enterprise Risk Management

Corporate security Resilience of the company

Platform Security

Optimizing the security of our clients' digital assets

Information and Cyber Security

Securing sensitive client business data & personal information

Transaction Security

Transaction and fraud monitoring

Our robust governance and risk management policies

Ceffu's top priority is to enhance customer confidence through strong governance and risk management capabilities.

Risk management framework

Ceffu's Risk Management Framework incorporates a governance structure that provides Board and Management-level oversight of its key risks, assigns ownership, roles and responsibilities, and allocates independent reporting lines. The Board of Directors and its sub-committees, namely the Nomination and Remuneration Committee, Audit Committee and Risk Management Committee, exercise independent oversight on Ceffu's risk strategies, tolerances and appetite, and ensure that an effective risk management framework, policies and resources are in place to achieve its business objectives.

The management team, led by the CEO, is responsible for implementing the strategies and policies endorsed by the Board, as well as the day-to-day operational decisions of the business. The management team comprises personnel with deep and broad local and international experiences across the digital assets industry, exchange operations and technology, as well as risk management and regulatory compliance.

The Management-level Enterprise Risk Committee reviews and recommends for Board approval the risk management policies relating to the key risks that Ceffu faces. The Head of Risk is responsible for overseeing the risk management function, ensuring that the custody of assets and any other ancillary activities are conducted in a safe and prudent manner.

Our 3 lines of defense

1. Revenue-generating and operational support functions
2. Oversight and advisory functions to validate and challenge existing controls and procedures
3. Independent audit function reporting to the Board of Directors

First line of defense: refers to revenue-generating and operational support functions responsible for executing day-to-day business and operational activities to achieve organizational goals and objectives, as well as implementing effective internal controls and procedures to manage relevant risks.

Second line of defense: refers to the oversight and advisory functions responsible to oversee risk management and advise the first line of defense in the setting up of controls and processes.

Third line of defense: refers to an independent audit function which provides assurance to the Board on the effectiveness of controls in the first and second line of defense.

Crisis management

Ceffu has also developed a crisis management, business continuity and IT disaster recovery program based on risk assessments conducted for various emergency and contingency scenarios to address business and technology resilience.

The Risk department is also responsible for the independent review and monitoring of Ceffu's risk profile on a periodic basis and reporting any significant vulnerabilities and risk issues to Management and the Board.

Operational risk

Operational risk includes risks arising from inadequate or failed internal processes and procedures, human errors as well as disruptions arising from external events. Such framework also includes an Operational Risk Management Policy that facilitates the control and mitigation of operational risks. Ceffu manages operational risks through establishing policies and procedures and controls to ensure safe operations. All departments are also expected to submit a monthly reporting on the operational errors that were committed during the month and the action plans that are put in place to prevent recurrence.

This program enables Ceffu to have appropriate levels of preparedness and resilience, as well as compliance with regulatory guidelines, in the event of disruptive incidents. The business continuity and IT disaster recovery plans are tested annually to ensure plan effectiveness and staff familiarity, and are updated as necessary based on testing results. Counterparty risks arising from service providers is covered under the Third-Party Risk Management Policy where business continuity capabilities of the outsourced service providers are assessed.

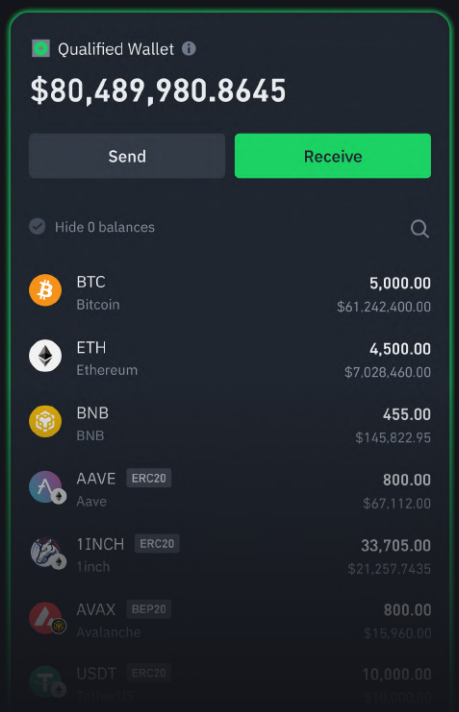
Ensuring institutional-grade security to safeguard client assets

Ceffu operates a separate, dedicated platform with segregated account and wallet systems. This means that client assets deposited in our cold wallet solution are never commingled with other clients' assets nor our own assets,

Each segregated account system comes with login risk controls, multi-factor authentication processes, multi-approval schemes for sensitive operations (such as address white-listing and withdrawals) and fraud prevention measures. All assets under our custody are covered by our cold storage specie insurance, which was obtained from Arch at Lloyd's of London after an independent evaluation of our security and risk management protocols.

Qualified Wallet

Using our Qualified Wallets, Ceffu clients maintain their own dedicated, on-chain wallet addresses which contain their funds only. This proof can be verified directly on the blockchain, as clients have full visibility and transparency that the only movements in/out of the wallet belong to them. There is no possibility for Ceffu to re-use client assets without their consent or knowledge. Asset ownership always remains with our clients.



Zero trust architecture

Building a 'trustless' platform that removes implicit reliance for each phase of our digital interaction is one of the main pillars in Ceffu's design. This setup significantly reduces risks of malicious insiders and bad actors from surreptitiously manipulating data, on top of eliminating single points of failure by combining Multi-Party Computation (MPC) cryptography with hardware isolation as our foundation to protect our clients' assets.

Key generation

Our key management solution is based on the Threshold Signing Scheme (TSS) and key shares are generated on separate, air-gapped FIPS 140-2 compliant devices. TSS is an MPC mechanism which requires M out of N (e.g. 3 out of 5) number of key shares to validate a transaction for signing. MPC works by splitting the traditional private keys into multiple pieces and distributing them in multiple places, ensuring that no one person has full access to the private key and that it is never reconstituted in full. Using geographically distributed Vault Devices the corresponding public key (and public address) is derived from the Key Shares. Outside of a key share Generation ceremony if a Vault Device is connected to WiFi, the Key Management App will automatically prevent any transaction signing.

Operational controls

Access controls to the Ceffu systems are controlled by pre-approved roles for approved users. All withdrawal transactions must be initiated by the user before they can be validated by analysts from Ceffu and can only go to client whitelisted wallet addresses (note: whitelisted means clients input the both wallet address and Ceffu address as whitelisted). On the user's side, in order to initiate a transaction, the request must also undergo the client's customizable multi-approval scheme in order to be confirmed.

Key storage

Key shares are stored in secure air-gapped FIPS 140-2 compliant devices. Locations of these devices are confidential and access to these devices require multi factor authentication and approvals. The key shares are managed by Ceffu analysts whose identities are confidential and transactions will only be signed once relevant compliance and risk checks are done.

Insurance and SAFU

Ceffu provides its clients with cold storage specie insurance, which protects against physical damage or loss of private keys, including employee misuse and theft. Our current insurance covers approximately 5% of our total assets under custody (AUC), which will scale as our AUC continues to grow and thus provide even greater protection. This insurance policy belongs to Ceffu. Ceffu clients are also eligible for Binance's SAFU (Secure Asset Fund for Users) monetary fund, which currently stands at US$ 1 billion.

Committed to information security and privacy protection

Ceffu has established a Technology Risk Management Framework based on industry-leading standards and best practices where technology-related risks are addressed by implementing policies, processes and controls on several key areas.

Information and cyber security policies

These include: network security, malware protection / anti-virus, patch management, user account management, privilege and passwords access controls, personal data protection, data loss prevention, security incident handling, cryptography standards, cloud security controls, refresh and disposal of storage media, employee awareness and training, among others.

Service management policies and procedures

These include: change and release management, incident management, problem management, system capacity management, data backups and restoration, disaster recovery (“DR”) and contingency plans to ensure the high quality and availability of Ceffu services.

IT project management and system development life cycle frameworks

These cover all phases from project initialization, planning, executing, controlling and closing.

Information classification and handling guidelines

These cover the proper classification and protection of confidential/highly sensitive data.

Management of third-party services

They address exposures to technology risks that may affect the confidentiality, integrity and availability of the IT systems and data at the third party.

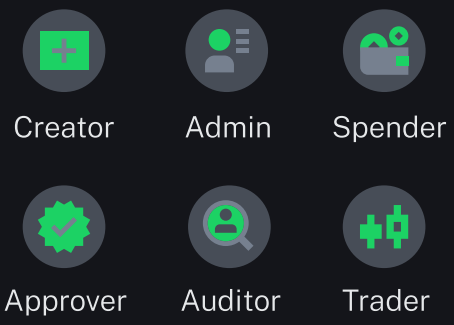
Our transaction and fraud management policies

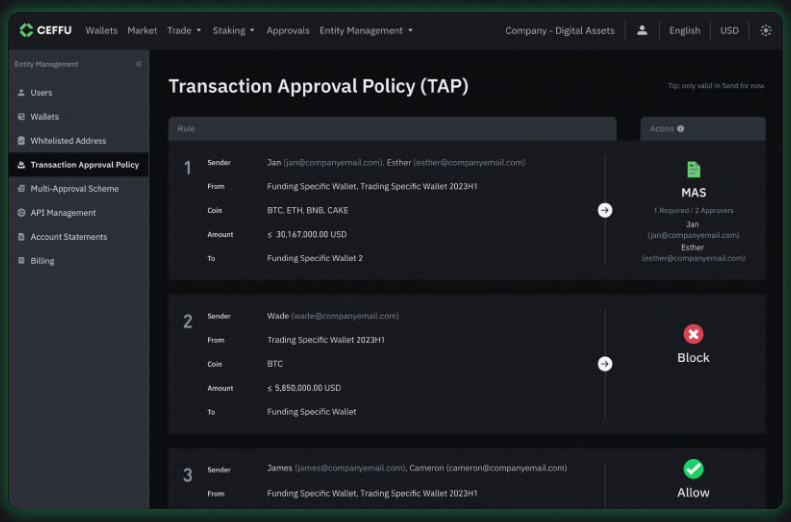
Ceffu uses authentication systems to encrypt and verify customers' credentials, including multi-factor authentication to verify customer identities. Transactions are monitored to ensure incoming deposits and withdrawals do not involve tainted wallets or assets that are involved in money laundering, sanctions, or any other prohibited activities.

Multisig framework

A multisignatory framework ensures that clients can customize their own M of N quorum based on their business needs and organizational structure. Our multisig infrastructure allows clients to set up a customized Transaction Approval Policy (TAP) for the onboarding of multiple persons onto the Ceffu platform, and to dictate the limits and boundaries of the movement of funds within their organization. Each person can be assigned a different role:

User roles





Whitelisted Wallet Addresses

Clients are required to define a whitelisted address for each wallet to limit the destination address of future withdrawal addresses. Only transfer to the address defined in the whitelist is allowed. This is to prevent fraudulent withdrawals.

Fraud Prevention

Time locks are built into our control systems, which Ceffu can activate to allow clients to prevent any pending errors or fraudulent transactions from being confirmed.

Entrust the security of your digital assets with our institutional custody platform.

We hold our custody platform to the highest standards of protection to provide our institutional clients with a safe, compliant environment that supports their needs of storing, managing, and utilizing their assets efficiently. With Ceffu as their trusted institutional custodian, our clients benefit from a wide range of innovative custody and deep liquidity products by way of our connectivity to the Binance ecosystem.

This secure access is made possible thanks to our highly resilient technology infrastructure, combined with our robust risk management framework, strong governance structure, and effective controls, providing institutions with peace of mind when entrusting the security of their assets with us.

For more information on how Ceffu can support your organization's digital asset needs, please reach out to **sales@ceffu.com**.