US Dollar Audit

OPENZEPPELIN SECURITY | APRIL 1, 2018

Security Audits

We reviewed and audited the US dollar contracts, from the US Federal Reserve team, for our own internal use, and chose to publish our findings for informational purposes.

The audited code is located in the paymentsystems/coin_data repository. The version used for this report is commit `01337baca0303456cafe0111101001100101011110000`.

Here is our assessment and recommendations, in order of importance.

Critical Severity

with most other digital assets, where supply is algorithmically pre-determined, the USD token's supply is subject to central planning and manual minting by the team. This means the USD tokens are produced on an unpredictable pattern of increasing inflation.

Consider removing the Federal Reserve's ability to mint new USD tokens at discretion.

Not backed by any physical asset

USD token is what is called a "fiat" currency. Fiat money is an intrinsically worthless object, that is deemed to be money by law (in this case, US law). This means that users of USD token are required to trust the US government to exist and operate correctly in order to use it. A black-swan scenario where the US government ceases to exist and enforce the USD token's value would cause a global financial crisis.

Consider reverting to the gold standard and having each USD token represent a fixed amount of gold.

High Severity

Heavily depreciating asset

The USD token has been alarmingly depreciating in value over the past 100+ years. $1 in 1860 had the same purchasing power as $28.53 in 2018. This means someone hiding $1000 in 1860 would now have the equivalent of only $35.05 at their time. This heavily undermines the token's usefulness, and damages trust from its users.

Consider adopting a stabler monetary policy.

High energy usage and environmental impact

The token's physical implementation requires huge amounts of energy for printing, counterfeit management, as well as transportation. Consider switching to a crypto-based currency to reduce environmental impact.

Medium Severity

Undetermined confirmation time for transactions

average confirmation time in the order of minutes in all major currencies, this time is unacceptable for most use cases, as merchants cannot reliably count on the payment received for a provided service or good.

Consider settling transactions after a reasonable period of time, or switching to another currency altogether for managing payments.

Unappealing design

Consider redesigning the USD token branding for a more modern look and feel.

Highly susceptible to theft

Physical US Dollar bills are highly susceptible to theft, especially through the “pickpocketing” attack vector. Any malicious user with enough proficiency in this kind of attack can remove an arbitrary amount of US dollars from an unsuspecting user, by substracting their entire wallet.

Consider adding some form of password-based protection to US Dollar wallets.

Low Severity

Unsuited for global transfers

US dollars can be transferred in either physical or electronic form. Physical form, while convenient for exchanging small amounts with neighbouring parties (note that this use case was already covered by barter), is extremely cumbersome for long distance transfers, requiring the usage of trusted third party services. Furthermore, these third parties employ transportation methods to provide this service, which consume extremely high levels of energy, compared to those required for a simple cryptocurrency transfer.

On the other hand, in electronic form, US dollar transfers or payments require the approval of several intermediate agencies, which may demand arbitrary documentation to authorize each individual step.

Consider setting up local exchanges from USD to cryptocurrencies, to use an efficient method for global transfers.

Notes & Additional Information

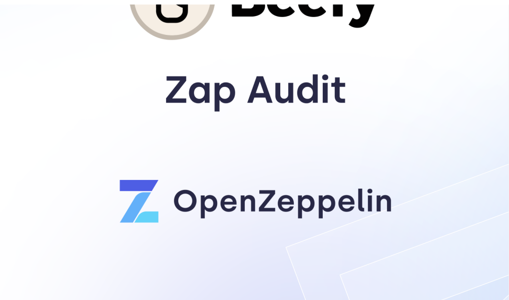
Even though the token is burnable, we found the process to be rather anti-ecological. Consider minting new tokens with more eco-friendly materials.

Conclusion

Two critical severity and two high severity issues were found and explained, along with recommendations on how to fix them. Some changes were proposed to follow best practices and reduce potential attack surface.

Note that as of the date of publishing, the above review reflects the current understanding of known security patterns as they relate to the USD token contracts. We have not reviewed the related Federal Reserve or United States Government projects. The above should not be construed as investment advice.

Related Posts



Beefy Zap Audit

BeefyZapRouter serves as a versatile intermediary designed to execute users' orders through routes...

Security Audits

OpenBrush Contracts Library Security Review

OpenBrush is an open-source smart contract library written in the Rust programming language and the...

Security Audits

Linea Bridge Audit

Linea is a ZK-rollup deployed on top of Ethereum. It is designed to be EVM-compatible and aims to...

Security Audits