WHITEPAPER

Document Version 2.0
March 2022
www.usd-z.com

THE USD ZEE: A NON-REGULATED STABLE VALUE COIN

Abstract.

The USD-Z is a cryptographic stablecoin that is (i) issued by a **ZEE SEE BUSINESS (PRIVATE) LIMITED** company, (ii) strictly pegged 1:1 to the U.S. dollar, and (iii) built on the Ethereum network, according to the ERC20 standard for tokens.

The USD-Z is a stable value coin that combines the creditworthiness and price stability of the U.S. dollar with the technological advantages of a cryptocurrency and the oversight of U.S. regulators. As an ERC20 compliant token, the USD-Z can be transferred on the Ethereum network. The USD-Z digital dollars are created at the time of purchase on the ZEE platform and redeemed or “burned” at the time of sale on the ZEE platform.

FORWARD LOOKING STATEMENT

For the purpose of full transparency, all statements contained hereunder, or any other statements made in press releases or in any place accessible to the public and oral statements that may be made by the USD-ZEE team or behalf of the USD-ZEE team by their legally appointed representatives in any given circumstance, constitute "forward-looking statements." However, this technical document is not the exclusive means of identifying forward-looking statements. Any other statement regarding USD-ZEE team's financial position, business strategies, plans and prospects, and future industry prospects made by USD-ZEE team are also considered forward-looking statements. These statements are matters that are not historical facts, but only predictions.

The predictions stated in this technical document, or in any other statements or publications may turn out to be wrong. Our assessments may, at any given time, be at least partially affected by inaccurate assumptions or by known or unknown present or unforeseen risks and uncertainties. Many such factors will be a determining factor to our actual future results. Consequently, no forward-looking statement can be guaranteed, and they may be adversely affected by tertiary elements, including general market conditions, national and international regulations and legislation, competitive product development, service availability issues, product availability, generic competition, timing of trades, patent positions, litigations, and investigations. We will have obligation to correct or update any forward-looking statements, whether because of new information, future events or otherwise.

So, our statements may involve potentially known and unknown risks, but also other factors that may cause USD-ZEE's actual future results, performance, or achievements to be materially different from our initial expectations. These factors include, but are not limited to:

a) changes in the political, social, economic, and stock market conditions or cryptocurrencies, and the regulatory environment wherever the USD-ZEE team carry out their businesses and operations.

b) the risk that the USD-ZEE team may not be able to execute or implement its respective business strategies and future.

c) changes in the anticipated growth strategies and expected internal growth of USD-ZEE.

d) changes in exchange rates and interest rates of cryptocurrencies and fixed currencies.

e) changes in the availability and salaries of employees required by the USD-ZEE team to operate their respective businesses and operations.

f) changes in user behavior and preferences of blockchain technology users or USD-ZEE holders.

g) changes in USD-ZEE team's future capital needs and the availability of financing and capital to finance such needs.

h) changes in the competitive conditions under which USD-ZEE team operate, and its ability to compete in such conditions.

i) Force Majeure events, such as natural disasters, wars or acts of terrorism, and any other cases that affect the business and / or operations of the USD-ZEE team.

INTRODUCTION

Cryptocurrencies have recently surged in popularity and investor interest. While they bear a promise perhaps as profound as the Internet itself, they suffer from substantial price volatility, thereby hindering their use as a medium of exchange and unit of account (two of the three functions of money). One proposed solution is the creation of a stable value coin (often called a "stablecoin"), whereby an issuer distributes a cryptographic token to customers in exchange for a specified fiat currency, like the U.S. dollar, at a fixed 1:1 exchange rate. Because the U.S. dollar is a highly desirable medium of exchange, as well as a globally accepted unit of account, it is a desirable peg for a stablecoin.

Several implementations of fiat-pegged stablecoins have been proposed, however, they all lack some combination of supervision, transparency, and examination As a result, doubts surrounding their solvency persist, as do concerns regarding the systemic risks they pose

What is needed is a stablecoin that people can trust. In this paper, we propose the USD ZEE, a regulated stablecoin that combines the creditworthiness and price stability of the U.S. dollar with the technological advantages of a cryptocurrency and the oversight of U.S. regulators.

TRUST

Building a viable stablecoin is as much of a trust problem as it is a computer science one. While Bitcoin created a system based on cryptographic proof instead of trust, a fiat-pegged stablecoin requires both due to its reliance on a centralized issuer.

Desirable outcomes in a system that relies (at least in part) on trust requires oversight. In the context of a stablecoin, we submit that the issuer must be licensed and subject to regulatory supervision.

From this, transparency and examination become requirements of the system, ensuring its integrity and engendering market confidence. We propose ZEE SEE Business (PRIVATE) LIMITED (ZEE),

PROOF-OF-SOLVENCY

One desirable outcome of a stablecoin is convergence between the tokens issued and the U.S. dollars exchanged for their creation. The amount of tokens issued and in circulation can be observed on the blockchain, however, verifying the underlying U.S. dollar balance to demonstrate proof-of-solvency requires examination by a trusted party. For assurance, we propose that the audit committee of the board of directors of ZEE engage an independent registered public accounting firm to regularly examine and attest to the underlying U.S. dollar balance in accordance with the attestation standards established by the American Institute of Certified Public Accountants.

CREATION, REDEMPTION, AND TRANSFER

A simple and elegant mechanism for creation and redemption is necessary to promote useability and encourage adoption. We achieve this by allowing ZEE customers to create and redeem USD-Z on the ZEE platform.

USD-Z are created when customers buy USD-Z with U.S. dollars on the ZEE platform. ZEE customers may exchange U.S. dollars for USD-Z at a 1:1 exchange rate by placing a buy order. The U.S. dollar amount of a buy order is debited from, and the corresponding ZEE digital dollar amount is credited to, a customer's ZEE account at the time of purchase. USD-Z are redeemed or "destroyed" when customers sell USD-Z for U.S. dollars on the ZEE platform. ZEE customers may exchange USD-Z for U.S. dollars at a 1:1 exchange rate by placing a sell order. The USD-Z amount of a sell order is debited from, and the corresponding U.S. dollar amount is credited to, a customer's ZEE account at the time of sale.

The USD-Z can be transferred on the Ethereum network.

CONTRACT SPECIFICATION

The specifications of the USD-Z require a network that allows for the development of decentralized applications (including smart contracts) that may be used to store and transfer value according to certain conditions set by the developer. The Ethereum network fulfills this criteria and has a technical standard for tokens, the 'ERC20' standard, which has experienced widespread, global adoption. As a result, there already exists a plethora of software and services that support ERC20 compliant tokens and provide access to and usability for end users (cf., Tether as originally built on Omni Layer, a protocol built on top of the Bitcoin blockchain). Alternatively, if the USD-Z were built as the native token of its own blockchain, it would take time for a similarly vibrant ecosystem of third-party developers and software to emerge. As a result, we have built the USD-Z as an ERC20 compliant token on the Ethereum network. Consequently, the USD-Z can be transferred on the Ethereum network and stored in any Ethereum address.

CONTRACT SEPARATION

As a Non-regulated issuer, we need a technical design and implementation that gives us the ability to upgrade the USD-Z stablecoin so we can:

1) Resolve vulnerabilities;
2) Extend the system with new features;
3) Improve the system and optimize its operational efficiency; and
4) Pause, block, or reverse token transfers in response to a security incident (i.e., catastrophic event) or if legally obligated or compelled to do so by a court of law or other governmental body.

We enable upgrades (the mechanism for which we describe in more detail below) by building a system of smart contracts that cooperate with each other. The core components of the USD ZEE system are three smart contracts that we refer to as ‘Proxy,’ ‘Impl,’ and ‘Store.’ The smart contract known as ‘Proxy’ is the public face of the USD-Z — it is the USD-Z’s permanent address on the Ethereum blockchain. There is, and will only ever be, one instance of ‘Proxy.’ It provides the interface with which token holders can interact and perform operations such as transferring tokens and viewing token balances; however, ‘Proxy’ contains neither the code nor the data that comprises the behaviour and state of the USD-Z. Instead, ‘Proxy’ delegates the right to execute the logic that governs token transfers, issuance, and other core features to the smart contract known as ‘Impl.’ In turn, ‘Impl’ does not directly control the data that constitutes the ledger of the USD-Z (i.e., the mapping of token holders to their balances); instead, it delegates ownership of the ledger to the smart contract known as ‘Store’ — the external and internal USD-Z.

CONTRACT CUSTODIANSHIP

For certain high-risk actions in the USD ZEE system, we need an offline approval mechanism. We, therefore, require each smart contract in the USD ZEE system to look to a custodian for approval. A custodian may be another smart contract or a keyset (online or offline). A custodian may look to another custodian, which may look to another custodian, and so forth, thereby creating a chain of custody or "custodianship." For instance, a smart contract may look to another smart contract, which ultimately looks to a keyset for approval. If a smart contract's custodianship terminates to an offline keyset, an offline approval mechanism for its actions has been created.

For example, 'Proxy' looks to a smart contract called 'Custodian,' which ultimately looks to an offline keyset for approval.

Likewise, 'Store' looks to 'Custodian,' which ultimately looks to an offline keyset for approval.

CONTRACT UPGRADES

Upgrading the USD-Z stablecoin is a high-risk action that utilizes the USD ZEE system's offline approval mechanism. To do this, we replace the current instance of 'Impl' by instructing 'Proxy' (via 'Custodian') to delegate active token implementation to a new instance of 'Impl,' and instructing 'Store' (via 'Custodian') to treat this new instance of 'Impl' as its single trusted source when accepting updates to the USD ZEE ledger.

Taken together, the custodianship of 'Proxy' and 'Store' makes USD ZEE system upgrades possible. In addition, custodianship itself can be upgraded. For example, if we need to change our offline keyset, we can instruct 'Custodian' to instruct 'Proxy' to look to a new instance of 'Custodian' that looks to a new offline keyset.

PRINTING TOKENS

Printing tokens is a high-risk action — the number of USD-Z issued and in circulation must never exceed the underlying U.S. dollar balance. We need a solution that provides the security of an offline approval mechanism yet the flexibility of an online approval mechanism. We propose a hybrid solution whereby the custodianship of 'Impl,' the smart contract that controls increases to supply of USD-Z stablecoins, involves both an online and offline approval mechanism. To implement this unique approach, we insert a smart contract called 'PrintLimiter' into the 'Impl' chain of custody.

With the approval of an online key, 'Impl' may print USD-Z up to an amount or "limit" as specified by 'PrintLimiter.' This limit may be increased with approval of an offline keyset (or decreased with approval of an online key). This solution gives the USD ZEE system the desired level of security and flexibility with respect to token issuance.

CONTRACT SECURITY

The USD ZEE system implements the following security features:

1) Offline Keys: Keys that approve high-risk actions are stored offline in ZEE's proprietary Cold Storage System.

2) Key Generation: Keys are generated, stored, and managed onboard hardware security modules (HSMs). We only use HSMs, each a “signer,” that have achieved a rating of FIPS PUB 140-2 Level 3 or higher.

3) Dual Control (Multisignature): High-risk actions require approval (i.e., digital signatures) from at least two signers. We utilize an M of N signing design, whereby M=2. This provides both security and fault tolerance.

4) Time Lock: Even after approval, high-risk actions are locked for a minimum period of time before being executed. This provides a grace period to detect — and preemptively respond to — potential security incidents.

5) Revocation: Pending actions can be revoked, allowing for the nullification of erroneous or malicious actions before being executed.

CONCLUSION

We have proposed a solution for a stablecoin that establishes trust through cryptographic proof and regulatory oversight. Our technical design is implemented on the Ethereum network. It includes an upgrade feature, an offline approval mechanism for high-risk actions, and a hybrid online-offline approval mechanism for token issuance that provides the desired level of security and flexibility. Our trust implementation involves linking licensed financial institutions and examiners to form a network of trust. Together, these implementations form the USD-Z, a regulated stablecoin that can serve as a viable medium of exchange and unit of account for centralized and decentralized applications.

LEGAL INVESTMENT DISCLAIMER

This Whitepaper is produced for informational and educational purposes only, and is not purposed as a financial promotion. The information, data, or analysis presented hereunder are NOT intended to form the basis of any investment decision. This document is not in-vestment advice, solicitation of any kind nor an endorsement. Nothing in this paper should be construed as an offer or inducement, or proposal for investment, that would determine the reader to engage in any form of investing activity, nor is it meant to be a sale or issuance of securities, interests, or assets.

The information in this technical document is provided in good faith. The USD-ZEE team expressly disclaims any and all responsibility, and readers, investors, expressly waive all claim for any direct or indirect loss or damages of any kind (whether foreseeable or not) arising directly or indirectly from:

- reliance on any information contained in this document or any information made available in connection with any further inquiries,
- any error, or inaccuracy in this document,
- any action resulting therefrom or
- usage or acquisition of the underlying asset.

USD-Z is a stablecoin and its purpose is only to enable the coin holders to undertake actions within the USD-ZEE platform. The project (USD-ZEE) is not a currency and should not be considered one by its holders. It must not be held or earned as a reward by any individual resident and/or citizen of a country in which holding such Tokens is illegal and/or in countries that consider such Tokens as securities. It is the readers responsibility to know the laws relevant to their legal jurisdiction and ensure they are compliant at all times.
As hereinabove stated, there are no guarantees that the USD-ZEE project and/or platform will succeed. There is no inherent monetary value associated with the USD-ZEE project, except of the one provided by the community.

We reserve the right to require all platform participants submit verifiable identity and residence documentation at any time in order for the USD-ZEE project to comply with our KYC and AML responsibilities. This may include validation of identity & residence documentation with an authorized third-party supplier, as well as ongoing monitoring.
Investors should seek professional financial advice regarding the appropriateness of investing in the project contemplated in this Whitepaper and should understand that statements regarding prospects may not be realized. Investors should note that the utility asset values may fluctuate. As always in the market economy, past performance does not guarantee future performance.

REFERENCES

[1] V. Buterin et al., “A next-generation smart contract and decentralized application platform,” https://github.com/ethereum/wiki/wiki/White-Paper, 2014.

[2] M. Hochstein, “Tether Confirms Its Relationship With Auditor Has 'Dissolved',” In CoinDesk, www.coindesk.com/tether-confirms-relationship-auditor-dissolved/, January 2018.

[3] N. Popper, “Warning signs about another giant bitcoin exchange,” In New York Times, https://www.nytimes.com/2017/11/21/technology/bitcoin-bitfinex-tether.html, November 2017.

[4] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” https://bitcoin.org/bitcoin.pdf, 2008.

[5] Ethereum Wiki, “ERC20 Token Standard,” https://theethereum.wiki/w/index.php/ERC20_Token_Standard.

[6] Tether. Tether: Fiat currencies on the Bitcoin blockchain. https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.pdf.

[7] National Institute for Standards and Technology, “Digital Signature Standard (DSS),” In Federal Information Processing Standards Publication 186-4, https://csrc.nist.gov/publications/detail/fips/186/4/final, July 2013.

NO ADVICE

Past performance is no guarantee of future returns and there is no guarantee that the market price of the Token will fully reflect their underlying net asset value. This Whitepaper does not constitute any investment advice, financial advice, trading advice, or recommendation by the USD-ZEE team. USD-Z is an open-source community stablecoin. Please realize that cryptocurrencies have the value that individuals associate with them.