ZeroStableCoin Whitepaper

Jeromy McDichael[⋆] Anatoli Smorin[⋆†] Hans Russellman[†]

[⋆] Stablecoin Technical University for Personal Inclusive Development
[†] Internet Radio AG, Zug, Crypto Valley, Switzerland

6th June 2022

Abstract

In human endeavour and in particular in the fields of romance and finance, users often ask rhetorical questions of the universe, such as "tell me why?" [BB99]. A common risk in decentralized finance when trading assets tokenized using digital ledger technologies is the need to maintain a stable peg against legacy physical assets known as "stuff". In this work we introduce what is to our knowledge the world's first run-proof, inflation-proof, recession-proof stablecoin, with built-in state-of-the-art rug pull and front-running mitigations. We call this revolutionary coin ZeroStableCoin (ZERC), which is a multi-chain, cross-chain, multi-layer crypto asset. ZERC achieves these unrivaled properties by being provably pegged 1:1 to $e^{i\pi} + 1$ pound sterling.

Contents

1 Introduction

Price is what you pay. Zero is what you get. — Crypto Warren Buffett

ZeroStableCoin is a human-focused and innovative stablecoin expanding blockchain technologies for a brighter tomorrow, deeply driven by an award-winning community. Unlike unstable stablecoins and unsafe safecoins, ZeroStableCoin's paradigm-shifting architecture transcends the legacy principles of finance to guarantee absolute constant stability and liquidity.

Indeed, the history of stablecoins is tainted with failed experiments, unauditable projects, and unstable stablecoins. Yet stablecoins are vital to the decentralized economy and the reliable operation of privacy-preserving, censorship-evading transactions across the universe. To restore trust in stablecoins, and provide the coin that Web3 deserves, we designed ZeroStableCoin (ZERC), the first stablecoin that is:

- Fully collateralized and auditable
- Post-quantum, post-P=NP, post-Singularity
- Immune to DeFi hacks and scams
- Zero-knowledge and fully private
- 100% MEV-proof and rug pull-proof
- 200% inflation-proof and run-proof
- Inclusive of all currencies: 1 ZERC = 1$ = 1£ = 1€ = 1 BTC
- Guaranteed no-questions-asked in every market and jurisdiction
- Free of oracles, order books, AMMs, LPs, or other risky mechanisms
- Multi-chain, cross-chain, layer 1- and layer 2-compatible

With such properties, ZeroStableCoin is an undisputable disruptor to the conventional financial system and a trailblazer in the digital use of traditional currencies.

1.1 The History of Money

Humanity has long used spherical objects made of metal as a store of value in order to conduct business [AlyBC]. Then came paper money, when humans got tired of carrying suitcases full of gold. But all paper money eventually returns to its intrinsic value – zero. Then came Bitcoin[Nak08], digital money (known in legal circles as "prosecution futures"[Seg14]) that is as unstable as ZeroStableCoin is stable.

In what we call the Dark Ages of Stablecoins, many "stablecoins" were created, but now have a value of zero or almost zero, or are widely believed to "go back to nothing", owing to their poor design or questionable governance model [Pfe22]. The Enlightenment of stablecoins has a name: ZeroStableCoin. the first coin that is *by design* pegged to zero, and is provably stable.

1.2 Related Work

Whereas we use zero to solve humanity's problems, other researchers have only used zero to attack cryptographic protocols [Qua21a; Qua21b] (ZeroStableCoin is provably immune to such attacks).

2 Use Cases: Securing DeFi, and More

ZeroStableCoin has many use cases, among which:

- **Securing DeFi**: ZeroStableCoin cannot be staked, locked, or swapped; no coin, no DeFi! No DeFi: no scams, no fraud! No scammers, no suckers!
- **Debanking the unbanked**: The unbanked banked by cryptocurrencies such as criminals, North Korea and individuals on sanctions lists, have the opportunity to not trade using ZeroStablecoin, free of the global US hegemony.
- **Automatic compliance with the US entity list** In debanking the unbanked and providing a store of value outside the reach of the US Government but simultaneously worth nothing, ZeroStableCoin ensures perfect compliance with United States Federal Regulations.
- **Making the world a better place**: With only ZeroStableCoin, crypto "investors" can stop crypto-investing and start enjoying life and invest in more valuable projects: relationships (studies show crypto investment is detrimental to human fertility [Ile22]), family, community support, art, and physical exercise.

3 The ZeroStableCoin Vision

3.1 Stablecoin Design

ZeroStableCoin is a collateral-based stable coin that can be deployed on any blockchain, be it as layer 1, 2, 3, or $n \in \mathbb{N}$, as a token with the symbol "ZERC". To protect the ZeroStableCoin users, the coin behaves as any standard transferable coin, except that ZERC is *untransferrable*—which also saves gas, and reduces our carbon footprint. For extra safety, ZeroStableCoin's total supply is set to 0, a defense-in-depth mechanism to prevent any deviation from the peg.

3.2 Proof of Stability

Our team of cryptographers and finance mathematicians proved the following theorem on the optimal value of the peg for a stablecoin:

Theorem 1. *There exists a $p \in \mathbb{C}$ such that a stablecoin pegged to p can be absolutely, infinitely stable, for p such that*

$$\sqrt{\sum_{k=0}^{\infty} \sin \frac{2\pi k}{6}} \leq p \leq \int_C f(z)dz$$

where C is an arbitrary closed contour of the holomorphic function $f : U \to \mathbb{C}$, with U some open region.

Proof. Left as an exercise. □

For simplicity and efficiency, we choose the value $p = e^{i\pi} + 1$ as ZeroStableCoin's peg, and a basis denomination in British pound sterling. The astute reader will notice, however, that the denomination choice is of little importance in our stablecoin's design, and that, in effect, any other denomination would be equivalent.

3.3 Empirical Resilience Evaluation

Our estimated readers, at this point, may object that object that stability in theory does not imply stability in practice, and they could not be truer. To address such concerns, we carried out a large number of simulations using our quantum computer, under various hostile market regime assumptions, and against different adversarial models: rational, irrational, malicious, honest-but-curious, honest-but-malicious, active, passive, proactive, probiotic, hermetic, and prophylactic.

Empirical results and further analytical evaluations demonstrated that ZeroStableCoin is highly unlikely to lose its stability, as long as it remains at a distance greater than $2GM/c^2$ from the nearest black hole, where G is the gravitational constant, c the speed of light, and M the mass of a holder's balance of ZERCs, bounded by $\mathsf{totalSupply} \times m$, where m is the mass of a single ZERC.

Our results are summarized in Figure 3.3, which show an aggregate of our quantitative models' results:

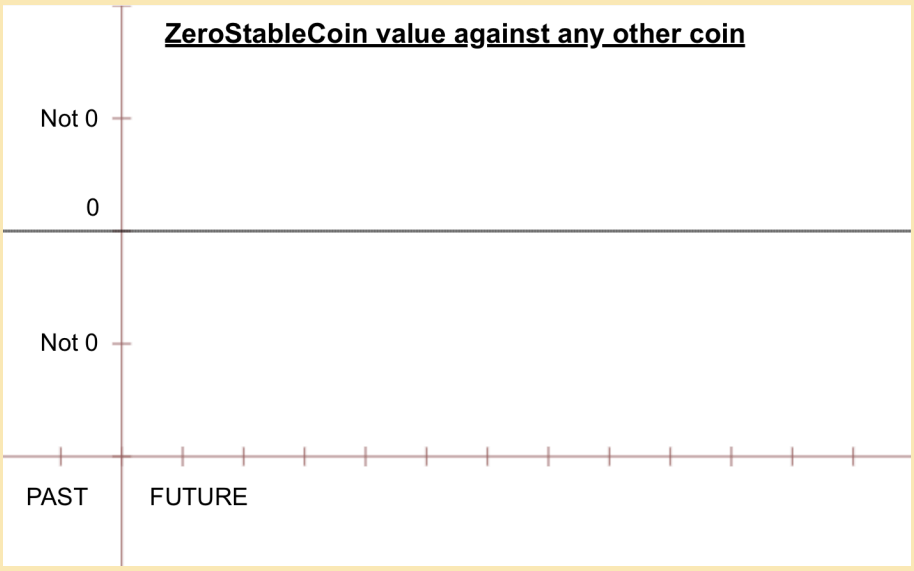

Figure 1: Quantitative analysis of ZERC value.

3.4 Value Analysis

Naive readers might be tempted to think that ZeroStableCoin is valueless, as zero is commonly associated with absence of value. However, the value of zero is non-null, though uncountable, as wiser souls than us demonstrated:

> *A zero itself is nothing, but without a zero you cannot count anything; therefore, a zero is something, yet zero.* — Dalai Lama XIV

ZeroStableCoin's emptiness of things is therefore its unparalleled power compared to other stablecoins. A power already discovered by philosophers specialized in the field:

> *Das Nichts nichtet.* — Martin Heidegger

3.5 Efficient Implementation for Web3

ZeroStableCoin is a multi-chain, multi-layer coin, that can run on any chain, such that all its functionalities can operate cross-chain with minimal latency and gas fees. Concretely, from an ERC-20 basis, ZeroStableCoin can be implemented with only the following methods:

```
function name() public view returns (string)
function symbol() public view returns (string)
function decimals() public view returns (uint8)
function totalSupply() public view returns (uint256)
function balanceOf(address _owner) public view returns (uint256 balance)
```

Owing to its size-optimized design, ZeroStableCoin is hightly gas-efficient, and straightforward to integrate in any layer-2 protocol:

- zk-rollup platforms do not require complex circuits or zkEVMs to support ZeroStableCoin.
- Optimistic rollup platforms can support ZeroStableCoin without suffering from long withdrawal delays.
- Layer 2 protocols with off-chain data can support ZeroStableCoin without worrying about data availability.

In terms of smart contract security, ZeroStableCoin offers unique defensive layers:

- Any attempt to fractionate ZeroStableCoin result in either an immediate halt of the underlying system, or an infinite loop conducting to its destruction.
- The total supply can be encoded in a single unsigned bit, making it almost impossible for attackers to manipulate it. Our experiments proved that in the worst case, it goes signed, but still hold its original value.

4 Risk Analysis

By design, ZeroStableCoin enjoys the following security properties:

- **Zero-knowledge and privacy-preserving**: even under worst-case assumptions, ZeroStableCoin cannot leak any transaction data or personal data.
- **Post-quantum and post-**P=NP: Quantum computers, even with qRAM, even if the polynomial hierarchy collapses, would fail to break ZeroStableCoin's peg. Event superintelligent sentient AI and alien civilizations from other galaxies couldn't break ZeroStableCoin, by the laws of physics.
- **Immune to front-running and MEV**: Owing to the zero value of the coin and to its untransferability, zero value can be extracted from transacting it or front-running transactions. QED.
- **Compliant with all regulations**: ZeroStableCoin's unique feature ensure full compliance with anti-money laundering, know-your-customer, cross-border payments, and other regulations and financial laws.

Furthermore, ZeroStableCoin is fully auditable and collateralized, as proven by our team of leading financial experts:

Theorem 2 (No undercollateralized minting)**.** *Neither rational nor irrational minters can initiate a new position that is undercollateralized.*

Proof. See the full version of this whitepaper. □

5 Future Work

ZeroStableCoin's vibrant community of developers, economists, and artists is already working on a variety of projects leveraging the ZeroStableCoin vision and technology. Among these, we can cite:

- ZeroNFT, an NFT that not only has zero value (as most NFTs), but a guaranteed price of zero.
- ZeroSwap, a fee-less coin swap service where any existing coin can be swapped again (zero) ZeroStableCoin.
- Zero-zero-knowledge proofs, a new type of succinct, non-interactive proofs that gains efficiency by minimizing eliminating "knowledge" to be zeroed.
- ZeroStableCOin derivatives, adapting the Black–Scholes model to consistently yield a price of zero.

To contribute to the ecosystem, please submit your grant proposal to the ZeroStableCoin Foundation.

References

[AlyBC] King Alyattes. *This is my coin!* http://rg.ancients.info/lion/article.html. 600 BC.

[BB99] Backstreet Boys. "I Want It That Way". In: *Millennium*. Ed. by Andreas Carlsson and Max Martin. Vol. Too Many. 1. https://youtu.be/watch?v=HlBYdiXdUa8. Jive Records, 1999.

[Ile22] Salem Ilese. "I don't care about your crypto, boy". In: (2022). Possibly the peak of human civilization. URL: https://www.youtube.com/watch?v=0amWsMfR2Ok.

[Nak08] Satoshi Nakamoto. *National Security Agency Tailored Access Operations*. 2008. URL: https://www.nsa.gov.

[Pfe22] Alexander Boris de Pfeffel Johnson. *Ministerial Code*. 2022. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1079310/Ministerial_Code.pdf.

[Qua21a] Nguyen Thoi Minh Quan. *0*. Cryptology ePrint Archive, Paper 2021/323. https://eprint.iacr.org/2021/323. 2021.

[Qua21b] Nguyen Thoi Minh Quan. *00*. Cryptology ePrint Archive, Paper 2021/1638. https://eprint.iacr.org/2021/1638. 2021.

[Seg14] David Segal. "Eagle Scout. Idealist. Drug Trafficer?" In: *The New York Times* (2014). URL: https://www.nytimes.com/2014/01/19/business/eagle-scout-idealist-drug-trafficker.html.