



CRYPTO TOFFE

CRYPTO TOFFE Let's explore the benefits of (CTP)

2023 - The Crypto Toffe Team

cryptotoffe.com

Unveiling Crypto Toffee's Revolutionary Blockchain Ecosystem

Crypto Toffee, the acclaimed platform that meticulously selects and presents the latest legitimate cryptocurrency airdrops, has reached a pivotal milestone. Introducing the Crypto Toffee Launch Coin (CTP), a native cryptocurrency token designed to elevate the airdrop experience and foster vibrant community engagement within the Crypto Toffee ecosystem. As we embark on this exciting journey with CTP, it is paramount to acquaint ourselves with the following important disclosures.

A Glimpse into the Future of Airdrops and Community Engagement

In the rapidly evolving landscape of cryptocurrencies, Crypto Toffee emerges as a trailblazing platform, reshaping how airdrops are experienced and how communities interact. Through the innovative (CTP) token, users are empowered with new dimensions of participation and value appreciation. This whitepaper will unravel the intricate architecture of the Crypto Toffee ecosystem, exploring its technical underpinnings, its integration with the Optimism network, and its commitment to providing sustainable rewards. Together, we'll dive into the visionary principles that drive this project and anticipate the future advancements that will further solidify Crypto Toffee's position at the forefront of blockchain innovation.

1. Introduction

In the digital era, cryptocurrencies have ignited a paradigm shift in how we envision financial systems and online interactions. At the heart of this transformation lies the innovative concept of blockchain technology—a decentralized, transparent, and immutable ledger that has unlocked countless possibilities across industries. Crypto Toffee harnesses this power to revolutionize the way cryptocurrency enthusiasts engage with airdrops and community-driven initiatives. With the introduction of the CTP token, Crypto Toffee establishes a bridge between traditional rewards and the exciting potential of blockchain, creating an ecosystem where participation is meaningful, and benefits are mutual.

(CTP) aims for full Ethereum- Optimism, allowing our rollup to support all existing Ethereum smart contracts and Dapps, developer tooling, and infrastructure. Complete compatibility benefits developers who can deploy their existing solidity contracts as is and continue using the tools they are familiar with. This compatibility also extends to network participants, finally it extends to end-users, who can experience the same usage patterns and continue using their preferred Optimism- Ethereum products.

2. Previous Work

Building upon its track record of excellence, Crypto Toffee has curated and promoted legitimate cryptocurrency airdrops since its inception. The platform's commitment to maintaining transparency and authenticity has earned it the trust of a burgeoning community seeking reliable opportunities in the crypto space. As a precursor to the CTP token, Crypto Toffee has fine-tuned its approach to ensure a seamless transition into this new phase of its journey. By learning from past successes and challenges, Crypto Toffee has paved the way for a robust ecosystem that aligns with the evolving needs of users.

3. Design Principles

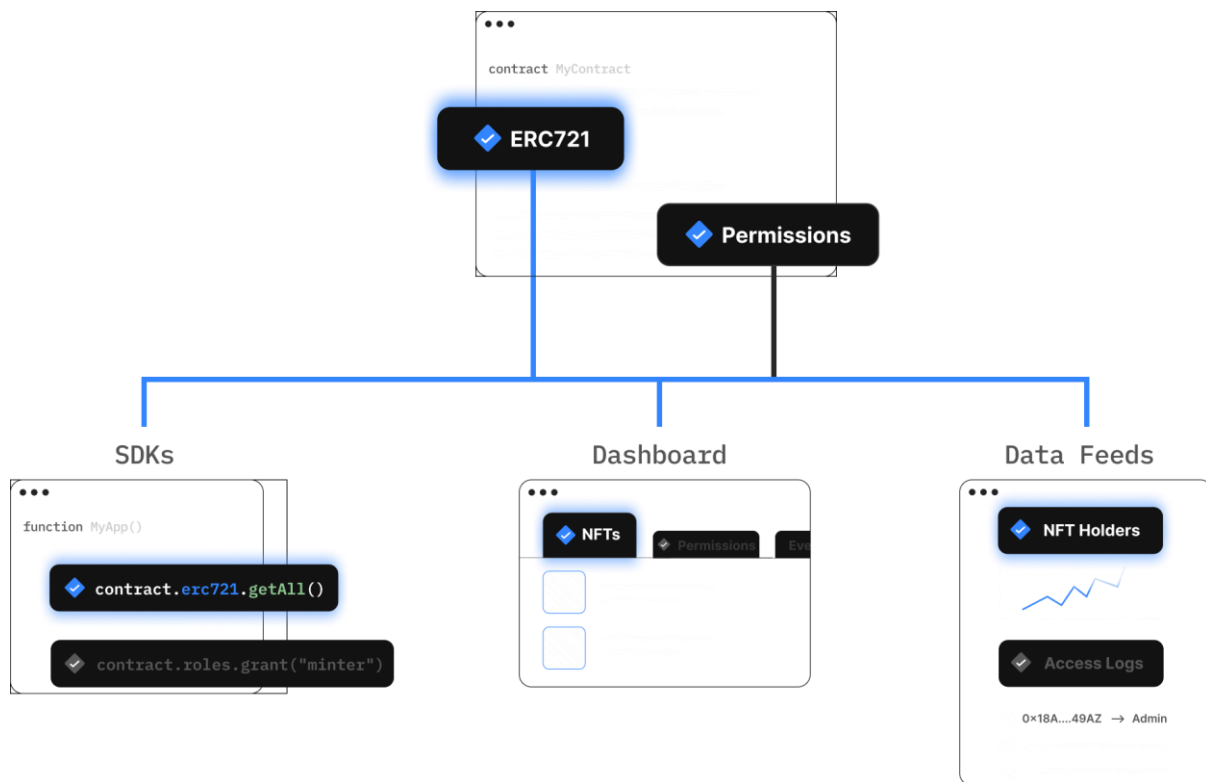
The design of the Crypto Toffee ecosystem is underpinned by core principles that drive every facet of its functionality. Transparency, accessibility, sustainability, and innovation constitute the pillars upon which the ecosystem stands. These principles guide decision-making, ensuring that the introduction of the CTP token not only enhances the user experience but also elevates the integrity of the platform. With a user-centric approach, Crypto Toffee embodies the spirit of blockchain technology, where decentralization empowers individuals to shape the direction of the ecosystem.

- **Secure.** The design should prioritize security above all else.
- **Minimal.** The design should be simple and focus only on the core third web protocol, not its upgradeability, governance, low-level optimizations, non-core bridging functionality, etc.
- **Robust.** The design should not depend on game theory for security. All security assumptions should be directly or indirectly enforced by Ethereum & Optimism protocol. For example, there should be no need to use a Proof-of-Stake-like system to slash participants for bad behaviour.
- **Decentralized.** The design should encourage a high degree of decentralization in terms of block proposing and proving. No single party should be able to control all transaction ordering or be solely responsible for proving blocks. Being sufficiently decentralized implies that the protocol should keep working in a reliable manner in adversarial situations.
- **Permissionless.** Anyone willing should be able to join and leave the network at any time, without causing significant disturbance to the network or being detrimental to the party in question. No single entity should have the power to allowlist or blocklist participants.
- **Ethereum-Aligned.** The goal is to help Ethereum scale in the best possible way.

4. Ecosystem Overview

The Crypto Toffee ecosystem is a dynamic hub where cryptocurrency enthusiasts, blockchain projects, and token holders converge to engage in a novel approach to airdrops and community participation. At its core, the ecosystem revolves around the CTP token, a utility token that embodies value, utility, and inclusivity. Through the seamless integration of blockchain technology, users can experience airtight security, real-time tracking, and frictionless transfers, all while participating in a community-driven environment.

- All block data required to reconstruct the post block state needs to be put on Ethereum, so it is publicly available. If this would not be the case, Taiko would not only fail to be a rollup but would also fail to be decentralized. This data is required so that anyone can know the latest chain state and so that useful new blocks can be appended to the chain. For the decentralization of the proof generation Taiko requires an even stronger requirement: all block data needed to be able to re-execute all work in a block in a step-by-step fashion needs to be made public. This makes it possible for provers to generate a proof for a block using only publicly known data.
- **Block proposal:** When a block gets proposed the block data is published on Ethereum and the block is appended to the proposed blocks list stored in the TaikoL1 contract. Once registered, the protocol ensures that all block properties are immutable. This makes the block execution deterministic: the post-block state can now be calculated by anyone. As such, the block is immediately verified. This also ensures that no one knows more about the latest state than anyone else, as that would create an unfair advantage.
- **Block verification:** Because the block should already be verified once proposed, it should not be possible for the prover to have any impact on how the block is executed and what the post-block state is. All relevant inputs for the proof generation are verified on L1 directly or indirectly to achieve deterministic block transitions. As all proposed blocks are deterministic, they can be proven in parallel, because all intermediate states between blocks are known and unique. Once a proof is submitted for the block and its parent block, we call the block on-chain verified.



5. The CTP Token and the Optimism Network

The CTP token serves as the backbone of the Crypto Toffee ecosystem, offering an array of benefits that extend beyond the realm of traditional airdrops. Leveraging the power of the Optimism network, CTP transactions achieve unparalleled speed and cost efficiency, ensuring that users can engage with the platform without limitations. As the community grows, so does the utility of the CTP token, creating a positive feedback loop that drives adoption and innovation.

Opcode Differences

Opcode	Solidity equivalent	Behaviour
COINBASE	block.coinbase	Undefined
DIFFICULTY	block.difficulty	Random value. As this value is set by the sequencer, it is not as reliably random as the L1 equivalent.
NUMBER	block.number	L2 block number
TIMESTAMP	block.timestamp	Timestamp of the L2 block

ORIGIN	<code>tx.origin</code>	If the transaction is an L1 \Rightarrow L2 transaction, then <code>tx.origin</code> is set to the aliased address of the address that triggered the L1 \Rightarrow L2 transaction. Otherwise, this opcode behaves normally.
CALLER	<code>msg.sender</code>	If the transaction is an L1 \Rightarrow L2 transaction, and this is the initial call (rather than an internal transaction from one contract to another), the same address aliasing behavior applies.
PUSH0	N/A	Opcode not supported yet (will be added in a hardfork)

`tx.origin == msg.sender`

On L1 Ethereum `tx.origin` is equal to `msg.sender` only when the smart contract was called directly from an externally owned account (EOA). However, on OP Mainnet `tx.origin` is the origin *on OP Mainnet*. It could be an EOA. However, in the case of messages from L1, it is possible for a message from a smart contract on L1 to appear on L2 with `tx.origin == msg.sender`. This is unlikely to make a significant difference, because an L1 smart contract cannot directly manipulate the L2 state. However, there could be edge cases we did not think about where this matters.

Transaction costs

EIP-1559

The L2 execution fee is calculated using EIP-1559 (opens new window). The cost of a unit of gas is composed of two components:

- Base fee: This fee is the same for all transactions in a block. It varies between blocks based on the difference between the actual size of the blocks (which depends on the demand for block space) and the target block size. When the block uses more gas than the target block size the base fee goes up to discourage demand. When the block uses less gas than the target block size the base fee goes down to encourage demand.
- Priority fee: This fee is specified in the transaction itself and varies between transactions. Block proposers are expected to select the transactions that offer them the highest priority fees first.

Parameter	OP Mainnet value	Ethereum value (for reference)
Block gas limit	30,000,000 gas	30,000,000 gas
Block gas target	5,000,000 gas	15,000,000 gas
EIP-1559 elasticity multiplier	block.number	L2 block number
TIMESTAMP	6	2
EIP-1559 denominator	50	8
Maximum base fee increase (per block)	10%	12.5%

Block time in seconds	2	12
Maximum base fee decrease (per block)	2%	12.5%

Blocks

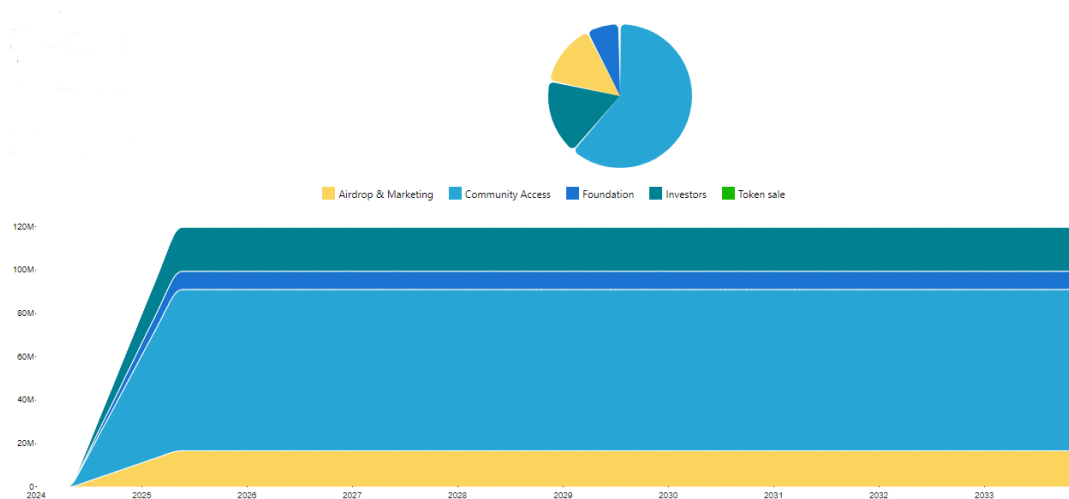
There are several differences in the way blocks are produced between L1 Ethereum and OP Mainnet.

Parameter	L1 Ethereum	Optimism Bedrock
Time between blocks	12 seconds ¹	2 seconds
Block target size	15,000,000 gas	5,000,000 gas
Block maximum size	30,000,000 gas	30,000,000 gas

6. Tokenomics

The total supply of (CTP) tokens is predetermined and fixed. This means that there is a specific maximum number of (CTP) tokens that will ever be created, ensuring scarcity and preventing inflationary issues.

Distribution



Category	Amount	Proportion
Total supply	120 Million	
Community Access	74 Million	62%
Investors	20 Million	17%
Airdrop & Marketing	17 Million	14%
Foundation	8.4 Million	7%
Token Sale	0	0

The initial distribution of (CTP) tokens occurred through a fair and transparent process. During the token does not open any sale or initial coin offering (ICO) phase, CTP tokens were made available to early supporters, investors, and participants who wished to be part of the Crypto Toffee project.

7. Sustainable Fees and Reward Mechanisms

Sustainability is a cornerstone of the Crypto Toffee ecosystem. To ensure its longevity and growth, a well-thought-out fee structure and reward mechanisms have been established. Transaction fees, meticulously designed to maintain affordability, contribute to the ecosystem's maintenance and enhancement. Simultaneously, reward mechanisms empower active participants by distributing CTP tokens based on engagement, fostering a vibrant and dynamic community.

8. Paving the Way for Future Advancements

As blockchain technology continues to evolve, Crypto Toffee remains committed to driving innovation and pioneering novel solutions. Future advancements encompass integration with emerging blockchain ecosystems, collaborations with innovative projects, and the expansion of utility for the CTP token. By staying agile and open to new possibilities, Crypto Toffee aims to set benchmarks for the blockchain industry while providing its community with unparalleled value.

- **Block Validity Verification at Proposal Time.** Currently we accept blocks at proposal time even if the transaction data is invalid. Afterwards, we depend on provers to generate a proof that shows the block is invalid (see Section 5.5.1). We do this because the work required to verify all requirements imposed on the transaction data is expensive to verify on L1. Instead, we can require a proof together with the proposed block attesting that the block data is valid.
- **Signature Compression.** Signatures can be removed from the block data as long as the proposer can show that all transactions in the proposed block have valid signatures. This can be achieved with the help of an accompanying proof when a block is proposed. As such, the burden of having to verify the signatures is shifted solely to the block proposer, so it needs to be possible to generate this proof efficiently. The block prover can then simply assume all transactions are valid and so there is no need for the prover to know the signatures. Note that this could have a very small impact on the transaction trie of a block as the signature data is not part of the transaction data anymore. If we want to keep the transaction trie the same with the signatures included the transaction trie will also have to be built by the block proposer.

EIP-1559 Powered Prover fees. Proving blocks requires significant compute power to calculate the proof to submit and verify the proof on Ethereum. Provers need to be compensated for this work as the network needs to attract provers that are willing to do this work.

9. References

The development and insights presented in this whitepaper are inspired by a multitude of reputable sources, including leading research papers, technical documentation, and industry best practices. This foundational knowledge ensures that Crypto Toffee's trajectory remains informed and aligned with the broader blockchain landscape.

1. <https://ethereum-magicians.org/t/a-rollup-centric-ethereum-roadmap/4698>
2. <https://eips.ethereum.org/EIPS/eip-2028>

3. <https://eips.ethereum.org/EIPS/eip-4844>
4. <https://github.com/privacy-scaling-explorations>
5. <https://vitalik.ca/general/2022/08/04/zkevm.html>
6. <https://github.com/taikoxyz/taiko-mono/tree/main/packages/protocol>
7. <https://ethereum.org/en/developers/docs/mev>
8. <https://ethereum.github.io/yellowpaper/paper.pdf>
9. https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm
10. <https://en.wikipedia.org/wiki/Deflate>
11. <https://github.com/ethereum/EIPs/blob/master/EIPS/eip-1559.md>
12. <https://dl.acm.org/doi/10.1145/3479722.3480987>

Disclaimer

The information provided in this whitepaper is intended for informational purposes only and does not constitute financial, legal, or investment advice. While every effort has been made to ensure the accuracy of the content, the creators of Crypto Toffee and this whitepaper cannot guarantee its completeness or reliability. Readers are advised to conduct their own research and seek professional advice before making any decisions based on the information presented herein.

The use of blockchain technology, cryptocurrencies, and related platforms carries inherent risks. The value of cryptocurrencies can be volatile and may result in significant financial loss. The creators of Crypto Toffee and the CTP token do not assume responsibility for any loss, damage, or inconvenience caused as a result of reliance on the information provided in this whitepaper.

By accessing and using the Crypto Toffee platform, readers acknowledge and accept the risks associated with blockchain technology and cryptocurrencies. The creators of Crypto Toffee reserve the right to modify, alter, or discontinue any aspect of the platform and its associated services without prior notice. It is the responsibility of users to remain informed of any updates or changes.

This disclaimer applies to the full extent permitted by applicable laws. Users are encouraged to review the terms and conditions of Crypto Toffee's platform for a comprehensive understanding of their rights and obligations.

