continuum

LIGHTPAPER

[v0.8.8] 08/12/2024

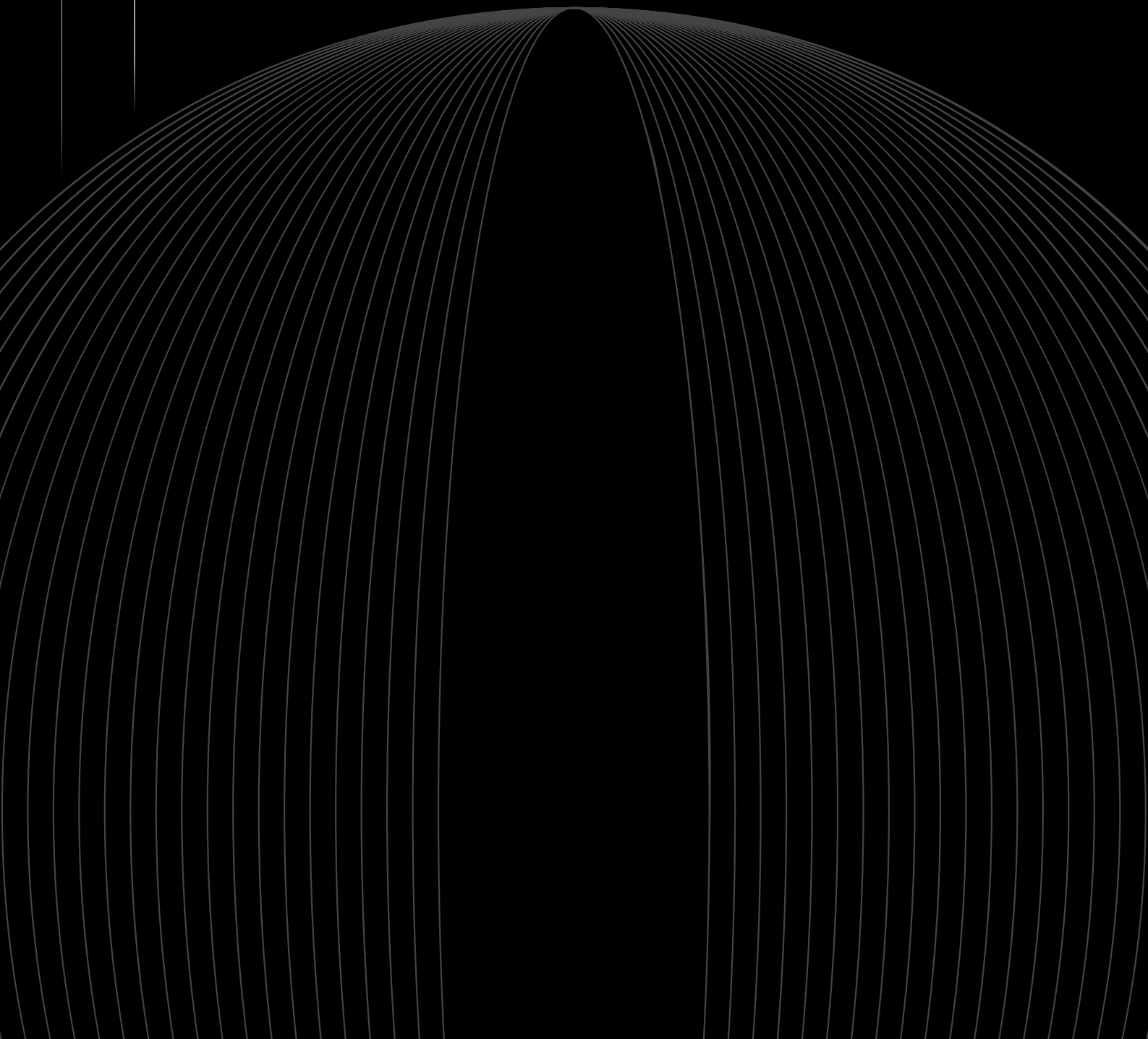
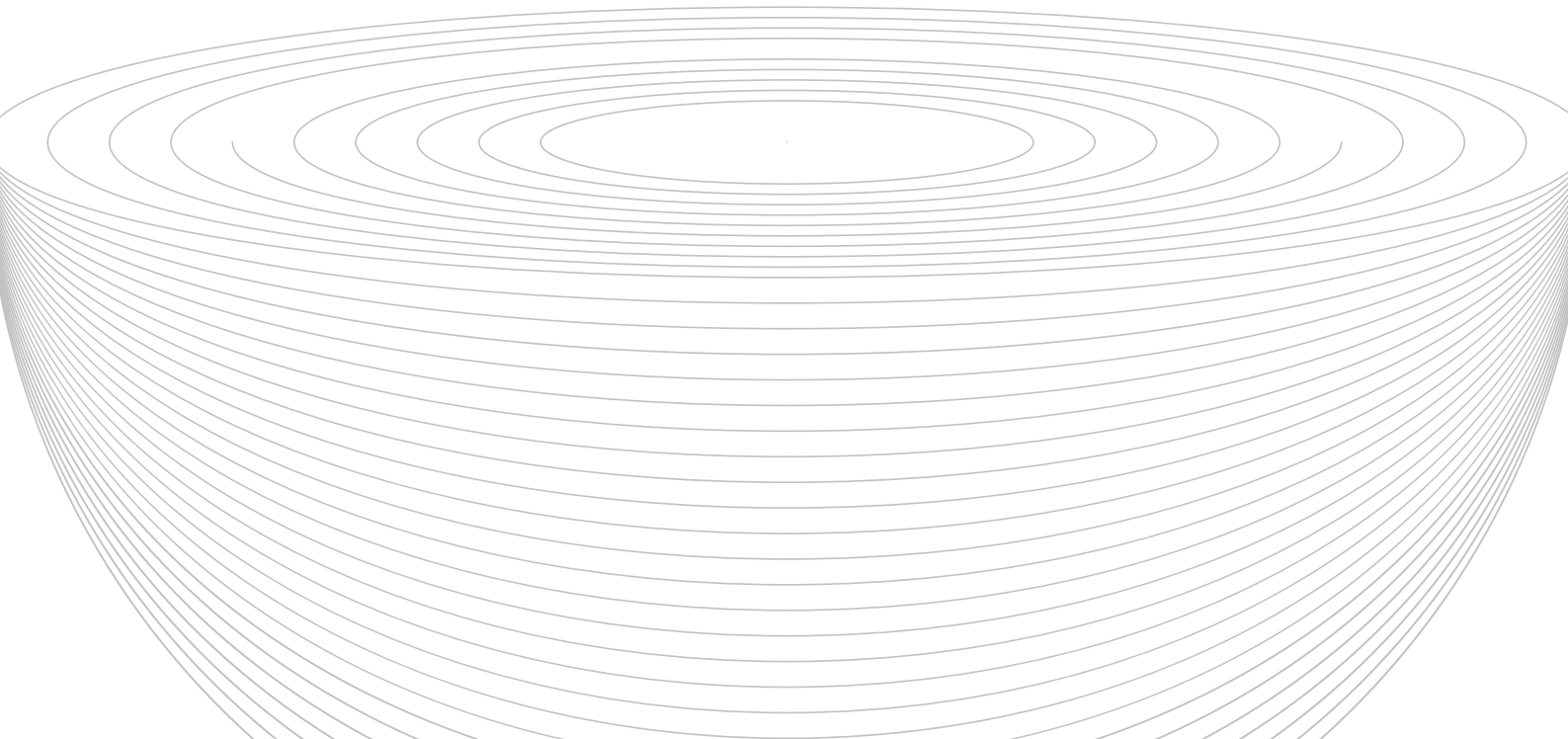


TABLE OF CONTENTS



I. INTRODUCTION

This lightpaper outlines the conceptual framework of the **c8ntinuum protocol,** its core mission, the problems it aims to solve, the proposed solution, and the unique features of its native coin, **CTM.**

Blockchain technology has revolutionized how we perceive digital ownership, trust, and consensus. However, the diversity of blockchain architectures has led to significant variations in capabilities and constraints. Issues such as scalability challenges, consensus mechanism limitations, and barriers in smart contract functionality have become prevalent, obstructing the seamless operation of decentralized applications.

Currently, blockchain networks are interconnected by either centralized providers such (exchanges) or quasi-centralized bridges susceptible to hacks, censorship, and other forms of third-party interference. These solutions are in general costly to operate and offer limited interoperability due to their monolithic structure.

The **space-time continuum** conceptually represents the integration of time and space into a single manifold. This analogy is applied to c8ntinuum to describe the seamless integration of blockchain networks, allowing for the dynamic flow of information and value across different times -historical, present, and future— and spaces—various blockchain ecosystems. This concept is the core idea behind c8ntinuum, a novel protocol aiming to connect and enhance the user experience for the next billion Web3 users.

c8ntinuum is a revolutionary **multi-chain protocol** designed to address the inherent limitations and challenges faced by existing blockchain networks.

The **blockchain trilemma** states that no blockchain network can simultaneously achieve all three properties: security, scalability, and decentralization. One property is sacrificed in favor of the other two. The blockchain trilemma can be represented as a triangle in 2D space. c8ntinuum aims to bypass this limitation by extending into another dimension: **interoperability**. Think of it as a 3D polyhedron where interoperability is the extra point in the model that is connecting the triangle shaped base.

c8ntinuum addresses these challenges by offering a flexible, multi-chain protocol that allows users and developers to navigate seamlessly across different blockchain networks. This integration facilitates the choice of the most suitable chain for specific needs, overcoming existing limitations and enhancing performance. By enabling seamless integration across leading blockchain platforms, c8ntinuum paves the way for blockchain networks to dynamically offload their weak points to others.

This creates an ecosystem where every chain maximizes its potential, offering an enhanced user experience for all Web3 users.

II. TECHNOLOGY

c8ntinuum is an **aggregated multi-chain interoperability protocol** that employs a trustless and permissionless infrastructure layer for transferring information and value between connected chains.

In the realm of blockchain interoperability, correct cross-chain communication is pivotal for ensuring that transactions and information exchanges between different blockchain networks are executed accurately and reliably. Correct cross-chain communication within c8ntinuum is designed to guarantee that all cross-chain transactions occur only with full consensus among involved parties, mirroring the principles of a fair exchange. This ensures that every transaction is not only effective and fair, ensuring all parties receive the outcomes they agreed upon but also timely, adhering to a predefined acceptable timeframe. This level of communication integrity is crucial for maintaining trust and efficiency in the c8ntinuum network.

It encompasses both a general message-passing framework and an asset transfer framework. Additionally, c8ntinuum features a novel, multi-chain **protocol-owned treasury** designed to continuously create value within its ecosystem.

Aggregation is a novel approach that combines the best of both worlds: the unified operation of a monolithic blockchain with the scale and efficiency of a modular blockchain stack.

Advantages compared to other interoperability solutions:

- **User perspective:** Unified, bridgeless UX
- **Developer perspective:** Seamless cross-chain interactions accessing user bases across multiple blockchain networks
- **Blockchain perspective:** Retain sovereignty without additional fragmentation

Multi-chain Interoperability

Interoperability is a spectrum of communication between different blockchain networks (L1s, L2s, etc.). One of the key properties of an interoperable ecosystem is asset portability.

The **fair exchange problem** is a fundamental issue in computer science and cryptography, particularly relevant in the context of blockchain interoperability. It involves ensuring that two parties can exchange digital assets in such a way that either both parties receive the items they expect, or neither party does. The challenge is to accomplish this without relying on a centralized trusted third party (TTP) to facilitate or guarantee the exchange.

The c8ntinuum protocol employs **trust-minimized cryptographic techniques** integrated into a decentralized and permissionless infrastructure to verify transactions and state changes across different blockchains without needing a centralized authority for coordination.

Interoperability Trust Gradients
Interoperability solutions can be classified based on their trust gradients, indicating the level of decentralization and security.

Proof-of-Authority (PoA) and External Decentralized Verifier Networks (DVN)
Uses private keys controlled by a central authority or information provided by external third parties (DVNs) to verify blockchain state and transactions.

- Examples: LayerZero, Chainlink CCTP
- Trust Level: Requires trust in the entities that run the DVN

Multi-Party Computation (MPC) and Threshold Signature Schemes (TSS)
Distributes the private key among a group of network participants using threshold signatures. It is a more decentralized approach than PoA if the TSS group is sufficiently large. However, scalability issues still arise when the TSS group is very large (i.e. more than 100).

- Examples: Thorchain
- Trust Level: Requires trust in the TSS group

Consensus Verification
Relies on the blockchain's own consensus mechanism to verify transactions. More decentralized and secure, as long as a significant portion of validators are honest.

- Examples: Axelar
- Trust Level: Requires trust in the validator set that runs the consensus.

State Verification
Uses cryptographic proofs, such as zero-knowledge proofs (zk-proofs), to verify the entire state of the blockchain. The highest level of security and decentralization, providing cryptographic assurance of state transitions without relying on any third-party intermediaries.
State verification is performed by on-chain zk-on-chain light clients where zero-knowledge proofs are used to provide cryptographic guarantees of state transitions.

c8ntinuum aims to provide the most trust-minimized way to achieve permissionless interoperability.

- **Decentralization:** By utilizing consensus verification, c8ntinuum ensures a higher degree of decentralization compared to MPC or PoA-based solutions.
- **Scalability:** c8ntinuum's consensus layer based on a modified version of CometBLS is decoupled to scale and support thousands of validators, enhancing the operation and security of the network.
- **Future-Proofing:** c8ntinuum's approach to state verification puts it in a pole position to achieve trustless and permissionless interoperability.

In summary, c8ntinuum addresses the limitations of traditional bridging solutions by focusing on consensus and state verification, thus providing a more secure, decentralized, and scalable approach to blockchain interoperability.

III. ARCHITECTURE

A typical modular blockchain stack divides the monolithic design into distinct layers as follows:

- **Execution layer**: Where transaction and state changes are executed.
- **Settlement layer:** An optional layer where execution layers verify proofs, resolve fraud disputes, and connect to other execution layers.
- **Consensus:** The layer where agreement on the order of transactions is performed.
- **Data availability:** Ensures transaction data is available for every participant.

c8ntinuum's design philosophy is based on a bridgeless architecture to achieve trustless and permissionless transfer of value or information between different blockchains, by leveraging cryptographic truth represented by zero-knowledge consensus proofs. This design is robust, yet modular. It does not require additional security assumptions beyond those of the underlying blockchain networks.

This approach does not rely on any external trusted third parties such as bridges, oracles, multi-signature or threshold-signature schemes.

One can think of it as a **universal aggregation layer** that has the following layers:

- **General data availability layer**
- **Settlement layer** for execution environments
- **Specialized zk-light-rollup** where the execution of the zk-light-clients is performed

c8ntinuum features a custom execution layer in the form of a specialized **zk-light-rollup** where zero-knowledge proofs of consensus are generated, a settlement layer where the validity of those proofs is verified, and a general data availability layer for ordering and efficient data retrieval. Trust-minimized bridging between rollups can be achieved only between rollups that share the same data availability layer. This approach follows the enshrined rollup design that shares the settlement layer to benefit from a trust-minimized "bridge" with it. Additionally, this benefits the ecosystem by having indirect trust-minimized bridging to other rollups that also enshrine bridges to this same settlement layer.

Basically, we reduce the bridging complexity, solving two important issues:

- The issue of **asset fungibility** that arises from bridging between many different blockchain networks
- The issue of **fragmented liquidity**

We have an alternative way to achieve all-to-all interoperability between connected chains and reduce the bridging complexity from to , without using one rollup as coordination hub: we take proof for all N chains, recursively aggregate all of them off-chain, then verify the aggregate zk-proof on each rollup independently. Now each rollup has a single proof for all rollups in this network.

Horizontal topology vs vertical topology
The flat topology contrasts with the hub-and-spoke model where you're bridging up and down through a single point. This allows you to eliminate the two-hop bridging process, but at an increased cost of off-chain execution.

Core Contracts
To communicate information between two blockchains without a trusted intermediary, we can simply verify the consensus of the source chain in the execution environment of the destination chain. zk-SNARK proofs can be used to prove that a certain consensus state transition has occurred on a blockchain. For example, a zero-knowledge proof can show that a transaction has been included in a block on chain B without revealing the transaction details. Smart contracts on chain A can verify the zk-proofs. If the proof is valid, the smart contract will trigger a specific execution depending on the type of swap mechanism that was implemented: lock-and-release or mint-and-burn.

zk-on-chain Light Clients
The principle behind light clients is to keep track of the state of a blockchain in a compute and storage-efficient manner. Light clients are designed to be computationally cheap to run to allow resource-constrained participants to be part of a blockchain network. However, they are not designed to be implemented as smart contracts: that's why we are developing custom zk-SNARK circuits to unlock gas-efficient on-chain light clients. Light clients embedded within blockchain *A* can verify the state of another blockchain *B* using zk-proofs. These light clients can verify state transitions with minimal data and compute footprint. zk-SNARKs enable a prover to efficiently convince *SC2* that a certain state transition occurred on chain *C1*. To achieve this, *SC2* tracks a digest *D* of the latest tip of *C1*. To sync *SC2* with new blocks in *C1*, anyone can generate and submit a zk-SNARK that proves the corresponding state transition to *SC2*.

c8ntinuum Relayers
At its core, a **c8ntinuum Relayer** operates as a modular execution engine with no persistent state and public key identifiers to securely exchange and relay data. The instructions it processes define methods for retrieving data from multiple blockchains, aggregating, and relaying messages back to the respective chains. To manage message storage and processing, c8ntinuum Relayers use a Kafka-based priority queue, leveraging Kafka's robust message handling and fault tolerance to ensure system reliability. The c8ntinuum Relayers are part of the **block header relay network** that actively listens to the state changes on the integrated chains and retrieves block headers from the full nodes. One key difference between existing solutions and c8ntinuum Relayers is that the trust assumption is reduced to the existence of a single honest node in the relay network and that the zk-SNARK circuits are sound.

c8ntinuum QTSS (Quorum-based TSS)
For blockchains without smart contract capabilities, TSS Quorums will manage asset custody in a decentralized manner. For example, a TSS Quorum based on FROST will be required to lock and unlock assets when certain events are emitted.

c8ntinuum ZKProvers
Zero-knowledge proofs solve the problems of a trustless and secure interoperable layer at the cost of computational bottlenecks due to large circuit sizes. The problem of computational overhead can be reduced using hardware acceleration. Since much of the processing is proving data-parallel circuits, a generalization of ZKP for parallelism like deVirgo is important.

IV. ECOSYSTEM SUSTAINABILITY

CTM, the native cryptocurrency of the c8ntinuum ecosystem, features a pioneering economic model characterized by a dynamic supply mechanism. This model, structured around a mint-burn equilibrium, is meticulously crafted to maintain sustainability and stability within the ecosystem. c8ntinuum's supply is capped at **8,888,888,888 CTM coins.**

The **generation of CTM** is driven by the permanent locking of whitelisted counter-assets into the protocol. During the Public Generation event, these counter-assets are allocated as follows: 40% is used to seed the liquidity pools, 10% is designated for referral incentives to boost participation and awareness, and the remaining 50% are re-staked by the protocol in participating blockchain networks to perpetuate ecosystem value generation. The resulting inflation generated via staking on the external chains is then utilized by the protocol to acquire CTM from the liquidity pools.

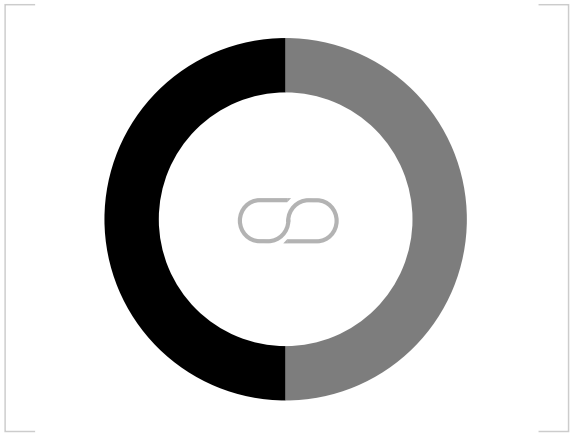
Embedded within the protocol are two positive feedback loops:

1. The External Value c8ntinuum Loop

This loop oversees the decentralized, secure management of pooled counter-assets. Its goal is to forge a positive feedback cycle by reinvesting assets to minimize risks. The additional value extracted from the counter-assets through staking (inflation on external networks) is converted back into CTM via the liquidity pools, with the ensuing CTM distribution as follows:

50%

allocated to c8ntinuum Validators to secure the network

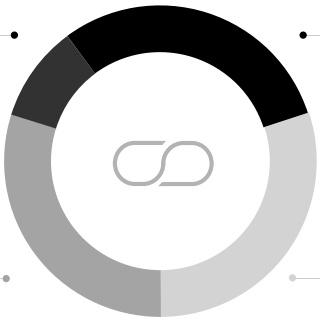


50%

burned to make room for future generations

2. The Internal Value Loop

At the core of the c8ntinuum protocol is the commitment to self-sufficiency. The protocol's execution fees are strategically utilized to encourage ecosystem engagement and expansion as follows:



10% allocated for interactive staking, a unique model where user interaction with a contract is required for staking

30% redistributed to active stakers, incentivizing consistent network participation and engagement

30% redistributed to Contract deployers (active developers), encouraging innovation and growth

30% redistributed to Validators, supporting network integrity

Interactive staking

Interactive staking is an innovative feature where users need to engage with a contract to stake their CTM, differentiating it from passive staking models where users lock up collateral in exchange for future rewards. Interactive staking within c8ntinuum transcends transactional activity, becoming an integral part of the user experience, inviting users to immerse themselves in the ecosystem.
This mechanism not only amplifies user engagement but also aligns individual interests with the overall health of the network. By necessitating active participation for staking rewards, c8ntinuum ensures that its members are consistently involved, contributing to and benefitting from the ecosystem's growth and dynamism.

All the mechanisms presented so far aim to cultivate a virtuous cycle, incentivizing users to actively engage with and advocate for c8ntinuum's long term growth, thereby driving participation and optimizing network efficiency. This staking model, exclusive to c8ntinuum, promotes active ecosystem involvement, ensuring that staking extends beyond mere passive income to foster genuine engagement and utility.

In essence, the dual loops of c8ntinuum establishes a robust framework for value creation, distribution, and retention, setting a new paradigm in the cryptographic and economic design of blockchain ecosystems. Through these innovative mechanisms, c8ntinuum aims to cultivate a thriving, self-reinforcing ecosystem that stands the test of time and fluctuating market dynamics.

The governance framework within c8ntinuum empowers the community to participate actively in the decision-making process, democratizing decision-making, and granting every CTM holder a voice in the evolution of the protocol. Through this inclusive approach, each CTM holder has the chance to influence the development of the protocol, ensuring that the direction of c8ntinuum is shaped by a dedicated and engaged community of Web3 pioneers.

V. CONCLUSION

c8ntinuum emerges as a groundbreaking solution, bridging the gaps between disparate blockchain networks through its innovative multichain protocol. By addressing the key challenges of scalability, interoperability, and functionality, c8ntinuum sets a new standard for the future of decentralized applications.

The introduction of CTM and its unique economic model further solidifies c8ntinuum's position as a pioneer in the blockchain space, promising a more interconnected, efficient, and user-centric decentralized ecosystem.

APPENDIX

A. Glossary of Terms

Aggregation: The process of combining multiple blockchain networks to function as a unified system, leveraging the benefits of both monolithic and modular blockchain architectures.

Asset Portability: The ability to transfer digital assets across different blockchain networks without losing their value or functionality.

Bridgeless Architecture: A system that facilitates the transfer of value and information between blockchains without the need for bridges, oracles, or multi-signature schemes.

Consensus: A protocol that ensures all participants in a blockchain network agree on the state of the blockchain.

Data Availability Layer: A layer in the blockchain architecture responsible for ensuring that all transaction data is accessible to participants.

Execution Layer: The layer where transactions are processed and state changes occur.

Light Client: A type of blockchain client that requires minimal resources to operate, typically used by participants with limited computational power.

Settlement Layer: An optional layer where execution layers verify proofs, resolve disputes, and connect to other execution layers.

Trustless: A system design where participants do not need to trust any single entity or intermediary because the system's security is maintained through cryptographic proofs and decentralized consensus mechanisms.

Zero-Knowledge Proofs: Cryptographic methods that allow one party to prove to another that a statement is true without revealing any additional information.

References

- zk-SNARKs: Groth, J. (2016). "On the Size of Pairing-based Non-interactive Arguments". EUROCRYPT 2016.
- Proof-of-Authority: Wood, G. (2017). "Ethereum: A Secure Decentralised Generalised Transaction Ledger". Ethereum Project Yellow Paper.
- Multi-Party Computation: Yao, A. C. (1986). "How to Generate and Exchange Secrets". FOCS 1986.
- Threshold Signature Schemes: Shamir, A. (1979). "How to Share a Secret". Communications of the ACM.

tags: Interoperability BlockchainLight clients Relay Network

DISCLAIMERS

Licences and approvals (if required) are not assured in all jurisdictions

c8ntinuum intends to operate in full compliance with applicable laws and regulations and use its best endeavours to obtain any necessary licences and approvals (if any). It is not possible to guarantee, and no person makes any representations, warranties or assurances, that any such licences or approvals will be obtained within a particular timeframe or at all. Moreover, laws and regulations evolve so c8ntinuum makes no guarantees, representations, or warranties that it will be able to obtain any necessary licences or approvals that may be implemented in the future. Accordingly, c8ntinuum may be required to restructure the Ecosystem Support initiatives and other activities described in this white paper or such services may be unavailable in all or certain respects in certain jurisdictions or may not be available at all.

No financial or investment advice

This lightpaper does not constitute any investment advice, financial advice, trading advice or recommendation by c8ntinuum, its affiliates, or its respective officers, directors, managers, employees, agents, advisors or consultants on the merits of purchasing any c8ntinuum supported tokens or interacting with any protocols available via the c8ntinuum network nor should it be relied upon in connection with any other contract or purchasing decision.

Not a sale of security

This lightpaper does not constitute a prospectus or financial service offering document and is not an offer to sell or solicitation of an offer to buy any security, investment products, regulated products or financial instruments in any jurisdiction.

No representations or warranties

No representations or warranties have been made to the recipient of this lightpaper or its advisers as to the accuracy or completeness of the information, statements, opinions or matters (express or implied) arising out of, contained in or derived from this lightpaper or any omission from this document or of any other written or oral information or opinions provided now or in the future to any interested party or their advisers. No representation or warranty is given as to the achievement or reasonableness of any plans, future projections or prospects, including with respect to the functioning or development of the c8ntinuum network or any applications thereof, and nothing in this document is or should be relied upon as a promise or representation as to the future. To the fullest extent possible, all liability for any loss or damage of whatsoever kind (whether foreseeable or not and whether or not c8ntinuum Labs has been advised of the possibility of such loss or damage) which may arise from any person acting on any information and opinions contained in this lightpaper or any information which is made available in connection with any further enquiries, notwithstanding any negligence, default or lack of care, is disclaimed.

Third party data

This lightpaper may contain data and references obtained from third party sources. Whilst the management believes that these data are accurate and reliable, they have not been subject to independent audit, verification, or analysis by any professional legal, accounting, engineering, or financial advisors. There is no assurance as to the accuracy, reliability or completeness of the data.

Translations

This lightpaper and related materials are issued in English. Any translation is for reference purposes only and is not certified by any person. No assurance can be made as to the accuracy and completeness of any translations. If there is any inconsistency between a translation and the English version of this lightpaper, the English version shall prevail.

Views of c8ntinuum

The views and opinions expressed in this lightpaper are those of c8ntinuum and do not reflect the official policy or position of any government, quasi-government, authority or public body (including but not limited to any regulatory body or self-regulatory body) in any jurisdiction. This lightpaper has not been reviewed by any regulatory authority.

Third party references

References in this lightpaper to specific companies, networks, protocols, technologies, and/or potential use cases are for illustrative purposes only. The use of any company and/or platform names and trademarks does not imply any affiliation with, or recommendation or endorsement of/by, any of those parties.

Graphics

All graphics included in this lightpaper are for illustrative purposes only. In particular, graphics with price references do not translate into actual pricing information.

Risk statements

Purchasing c8ntinuum-supported tokens or interacting with c8ntinuum-supported applications or protocols involves substantial risk and may lead to a loss of a substantial or entire amount of the money involved. Prior to purchasing c8ntinuum-supported tokens or interacting with c8ntinuum-supported applications or protocols, you should carefully assess and take into account the risks, including those listed in any other documentation. A purchaser should not purchase c8ntinuum-supported tokens for speculative or investment purposes. Purchasers should only purchase c8ntinuum-supported tokens if they fully understand the nature of the c8ntinuum-supported tokens and accept the risks inherent to such tokens, their relevant applications and protocols, and the c8ntinuum network itself.

Cryptographic tokens may be subject to expropriation and/or theft; hackers or other malicious groups or organizations may attempt to interfere with the c8ntinuum network or relevant applications or protocols in various ways, including malware attacks, denial of service attacks, consensus-based attacks, Sybil attacks, smurfing, and spoofing which may result in the loss of your cryptographic tokens or the loss of your ability to access or control your cryptographic tokens. In such event, there may be no remedy, and holders of cryptographic tokens are not guaranteed any remedy, refund, or compensation.

The regulatory status of cryptographic tokens and digital assets is currently unsettled, varies among jurisdictions and is subject to significant uncertainty. It is possible that in the future, certain laws, regulations, policies or rules relating to cryptographic tokens, digital assets, blockchain technology, or blockchain applications may be implemented which may directly or indirectly affect or restrict cryptographic token holders' right to acquire, own, hold, sell, convert, trade, or use cryptographic tokens.

The uncertainty in tax legislation relating to cryptographic tokens and digital assets may expose cryptographic token holders to tax consequences associated with the use or trading of cryptographic token.

Digital assets and related products and services carry significant risks. Potential purchasers should take into account all of the above and assess the nature of, and their own appetite for, relevant risks independently and consult their advisers before making any decisions.

Professional advice

You should consult a lawyer, accountant, tax professional and/or any other professional advisors as necessary prior to determining whether to purchase c8ntinuum-supported tokens or operate applications on top of the c8ntinuum network.

Caution Regarding Forward-Looking Statements

This lightpaper contains certain forward-looking statements regarding the business we operate that are based on the belief of c8ntinuum as well as certain assumptions made by and information available to c8ntinuum. We do not purport to make any statements with respect to the conduct or operations of any third parties whose actions (including commercial activity) may affect the c8ntinuum network. Forward-looking statements, by their nature, are subject to significant risks and uncertainties. Forward-looking statements may involve estimates and assumptions and are subject to risks, uncertainties and other factors beyond our control and prediction. Accordingly, these factors could cause actual results or outcomes that differ materially from those expressed in the forward-looking statements. Any forward-looking statement speaks only as of the date of which such statement is made, we undertake no obligation to update any forward-looking statements to reflect events or circumstances after the date on which such statement is made or to reflect the occurrence of unanticipated events.

R E A C H

c8ntinuum

c8ntinuum is an organization of worldwide professionals driven by a vision for a connected future.