QUAI NETWORK

Quai Network: Reignite the Crypto Revolution

The first decentralized energy dollar on the only scalable and programmable Proof-of-Work blockchain.

QUAI NETWORK

Table of Contents

Introduction

BACKGROUND

Cryptocurrency has demonstrated the potential to revolutionize money, the economy, and society. Despite this potential, blockchains are constrained by limitations in scalability. Low throughput causes high fees preventing broad adoption of decentralized systems outside of small niche use cases. Current attempts at scaling blockchains do so by sacrificing decentralization and removing the properties of neutrality and immutability. Once trust is reintroduced, blockchains' primary value proposition, trustless digital value transfers is lost.

A decentralized high throughput blockchain will allow cryptocurrency to not just be used as a store of value, but also as a unit of account & medium of exchange which is required for everyday commerce. This will allow cryptocurrency to replace the current fiat denominated monetary system and liberate money from the state.

THE QUAI VISION

Imagine a world where all global economic activity occurs on blockchain. This vision represents the original goals of cryptocurrency: decentralization, privacy, and freedom from centralized control. It's a world where individuals are empowered to openly transact without intermediaries and where the financial system is transparent, secure, and fair.

Imagine a blockchain that:

- Is ubiquitous and standardized as TCP/IP.
- Secures the majority of global value.
- Has native financial instruments.
- Is used for everyday transactions.
- Is open, accessible, and credibly neutral for everyone.

This vision is rooted in the core principles of the cypherpunk movement and focuses on using cryptography and game theory to bring societal change and protect individual liberties. It's about creating a system where trust is established through code, not institutions, and where financial sovereignty is guaranteed for all people. The Quai Vision is one in which blockchain technology extends beyond niche speculative use cases and empowers us to take control of our financial destinies.

In this future:

1. Individuals have full control over their assets, which cannot be censored or confiscated.
2. Smart contracts replace financial institutions and intermediaries.
3. Decentralized finance (DeFi) protocols provide accessible financial services to anyone with an internet connection.
4. Digital identities are self-sovereign, allowing people to manage their personal data and decide how it's shared.
5. Optionally transparent and immutable record-keeping enhances accountability in both public and private sectors.
6. Cross-border transactions occur instantly and at a fraction of the cost, accelerating global trade and remittances.
7. Tokenization of real-world assets creates new investment opportunities and increases liquidity in traditionally illiquid markets.
8. Decentralized governance models enable more direct participation in decision-making processes, from corporate management to public policy.

This vision imagines a global economy built on the principles of individual sovereignty and prosperity through Laissez Faire economics.

THE QUAI NETWORK

In this paper, we propose Quai Network, a blockchain designed to function as a new global monetary system.

Quai Network has the following characteristics:

1. **Scalability to Meet Real-World Demand:** Throughput of 50,000 transactions per second (TPS).
2. **Non-Fiat Dollar-Equivalent:** An energy dollar with cash-like properties that is not tied to traditional fiat currencies.
3. **Programmable Finance Layer:** An EVM smart contract ledger that enables complex financial logic on-chain.
4. **Proof-of-Work:** Secured through the only economic, immutable, consensus mechanism Proof-of-Work.

MONEY FOR THE 21ST CENTURY

Throughout history, money has evolved to reflect the dominant resource of each era. From agricultural commodities to precious metals, and finally to fiat currencies, each form of money mirrored the economic realities of its time. Now, as we transition into a world where information and energy are the primary drivers of value creation, Quai introduces a new form of money tailored for this digital age.

The increasing importance of information and energy in our daily lives necessitates a monetary system that reflects these new realities. Quai is designed for the world we inhabit now, not the world of the past. This implies:

Global Payments: Quai enables truly global, low-cost, decentralized payments, addressing limitations that have hindered widespread adoption of cryptocurrencies.

On-Chain Systems: Quai allows for the development of on-chain systems that were previously limited by technological constraints. This opens up possibilities for decentralized versions of services that were previously impossible.

Energy-Based Currency: In a world where energy is the base asset of the economy, an energy-based dollar becomes not just innovative, but necessary.

NEW STABLECOIN ALTERNATIVE CATEGORY

By tethering value to energy expenditure via Proof-of-Work mining, Quai creates a non-fiat, energy-based money. This isn't just a new cryptocurrency; it's a fundamental reimagining of what money can be in a world where bits and joules are as vital as dollars and cents.

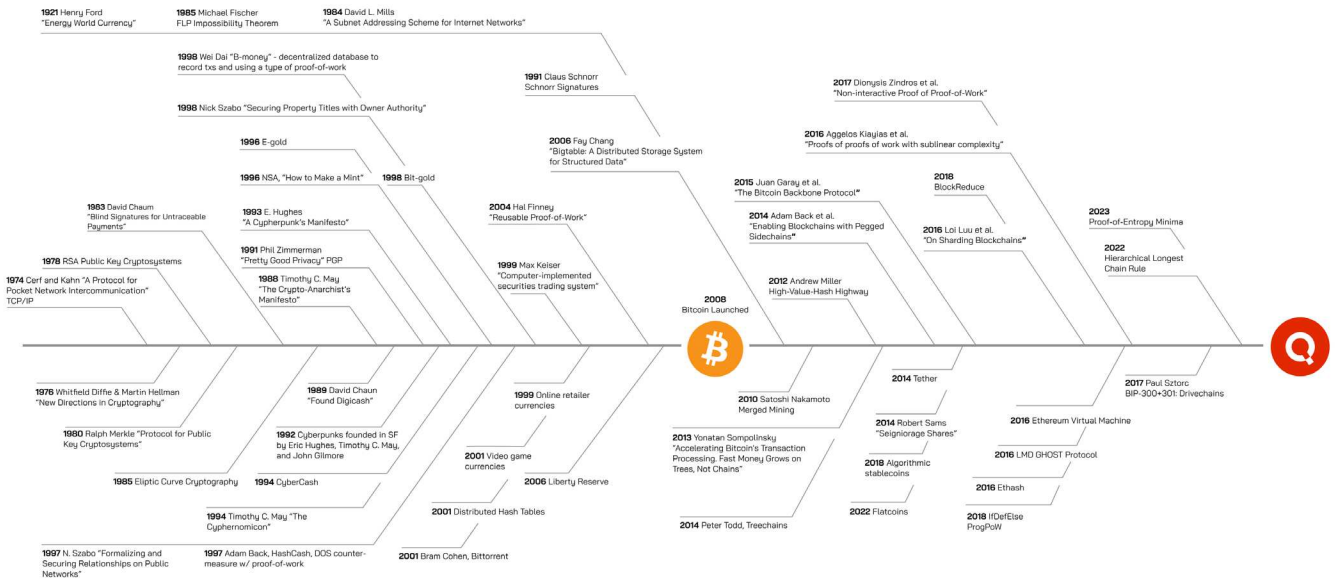
A TRUE MEDIUM OF EXCHANGE

Quai bridges the gap between traditional cash and digital payments by offering cash-like properties in a digital format. It enables fast, low-cost transactions without compromising on privacy or decentralization.

This approach addresses many of the concerns surrounding both traditional cash (such as physical limitations and security risks) and existing digital payment systems (like accessibility concerns and centralized control). Quai offers a best-of-both-worlds solution, combining the acceptability and usability of cash with the efficiency and global reach of digital payments.

FUTURE-PROOF TECHNOLOGY

Quai represents the next evolution in blockchain architecture, moving from monolithic to multi-threaded designs. It balances horizontal and vertical scaling, integrating modular components into a cohesive, integrated system. This approach incorporates and advances the blockchain timeline from Bitcoin's inception to a new paradigm of scalability and efficiency.



Quai - Blockchain Beyond Bitcoin

By addressing the blockchain trilemma (decentralization, security, and scalability) in novel ways, Quai paves the way for blockchain technology to handle global-scale operations without sacrificing its core principles. This could enable blockchain to finally achieve its potential as a foundational technology for the global digital economy.

Network Overview

Quai is a massively scalable secure blockchain network for fast, low-cost, high-throughput transactions and programmable smart contracts, while ensuring fast finalization, censorship resistance, and adversarial resilience.

The system is built using an integrated multi-threaded approach with adaptive architecture and two native cryptocurrency coins, all enabled by the breakthrough Proof-of-Entropy-Minima (PoEM) consensus mechanism. These features evolve from and draw inspiration from over 50 years of cryptographic and technological development.

One of the key differences for Quai Network is that it uniquely relies on the objective computational properties of Proof-of-Work to push the boundaries of blockchain performance. As a work-based consensus algorithm, PoEM removes the following performance, security, and access constraints found in Proof-of-Stake blockchains:

1. **Signature aggregation overhead, block message rounds**
2. **Nothing at stake attacks**
3. **Posterior attacks**
4. **Lack of energy commitment**
5. **Cold-start decentralization and distribution**
6. **Liveliness guarantees**

By innovating in an often overlooked area of research, Quai Network has been engineered with unique network properties that are significantly more advanced than existing solutions. In practice, this means that Quai Network can reach an impressive 1k TPS per shard and over 50,000 TPS in total (~1 gigagas/s). This is done by two distinctive forms of scaling:

- **Vertical scaling:** Maximizing the capabilities and performance of each individual shard.
- **Horizontal scaling:** Adding more capacity to the overall network once prior existing shards cannot service demand.

VERTICAL SCALING

ITEM	IMPROVEMENT
PoEM Consensus	Improves time to finality by 26% compared to vanilla Proof-of-Work via single round communication.
Self-organized Subnets	Reduces latency and ping times (<100ms) within a closely coordinated set of nodes. Blockchain throughput is limited by data propagation latency.
Workshares	Faster finality with higher hash sample rate. Worked object that is DDoS protected to efficiently transmit groups of transactions. Reduces impulsive bandwidth by 100x - 1000x.
State-rent	Minimizes overhead from unused accounts.
Dust Collection	Dust collection in Qi allows for a very large but sustainable UTXO set.
Parallel TX Processing	Enforced access lists create structured dependencies allowing for the processing of EVM state to be parallelized.

HORIZONTAL SCALING

ITEM	IMPROVEMENT
Horizontal Sharding	Dynamic horizontal sharding enables greater throughput on the network at the cost of cross-chain settlement time.
Sharded Clients	Allows machines to run subset of shards in order to reduce overhead and decrease propagation latency.

Benefits of being all-in-one as opposed to relying on multiple layers is that network growth is not stunted due to capacity constraints or L2 fragmentation.

Beyond high performance, Quai Network utilizes many improvements in accessibility that allow it to remain decentralized while functioning at scale.

ACCESSIBILITY / QUALITY OF LIFE

ITEM	IMPROVEMENT
NiPoPoWs	Non-Interactive Proofs of Proof-of-Work allow for proving of state history and fast sync times
UTXO Ledger	Both account and UTXO ledgers for different representation of assets
ETXs	ETXs enable trustless cross-shard transactions
EVM	EVM-compatible enables access to the largest dApp developer community
ProgPoW	ProgPoW is an ASIC resistant mining algorithm

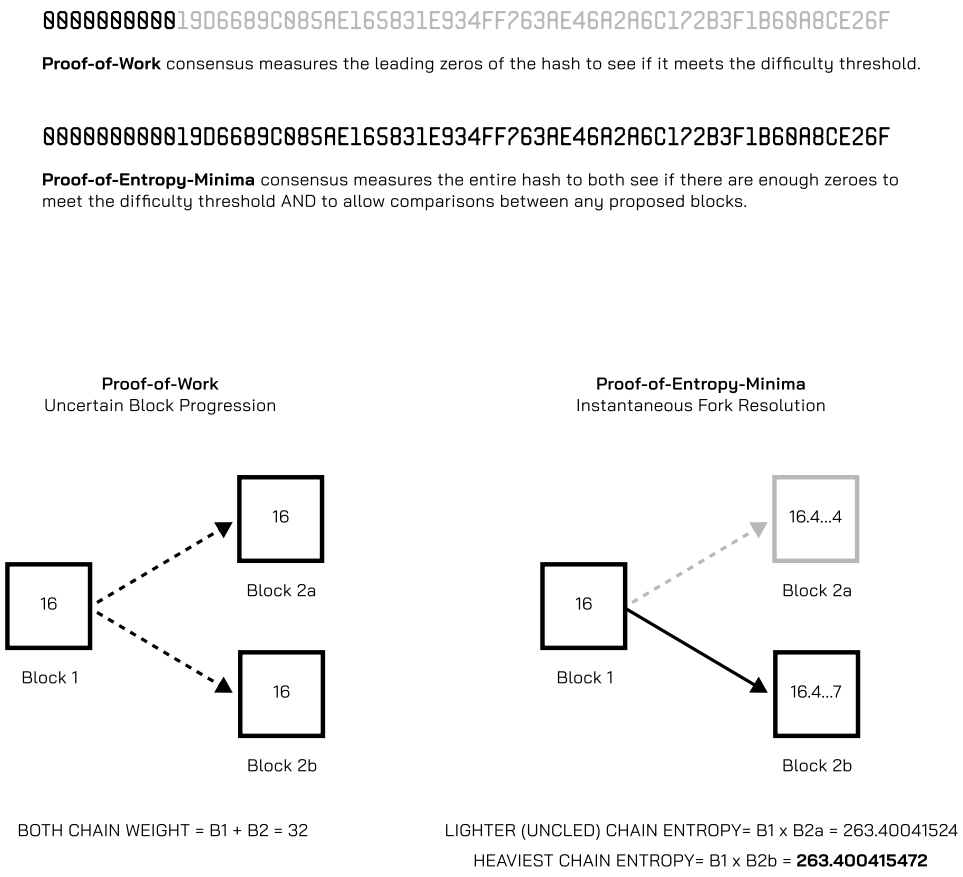
POEM CONSENSUS

Bitcoin's Nakamoto consensus mechanism pioneered the ability to achieve agreement in distributed ledgers through the heaviest chain rule (HCR). HCR determines which chain is canonical by summing cumulative block difficulty thresholds. However, this approach doesn't account for the actual achieved difficulty (the value beyond the threshold), leading to indeterminism in block choice thus delaying finality. To address these issues, we have introduced a new mechanism called Proof-of-Entropy-Minima (PoEM), which incorporates intrinsic block weight by considering the entire entropic reduction achieved by the work applied to a valid block. PoEM reduces the orphan rate and accelerates finalization, providing a causally invariant time-independent weighting of blocks in the chain.

Nakamoto consensus with HCR often results in orphaned blocks due to network propagation delays, leading to inefficiencies and wasted work from the associated Proof-of-Work (PoW) algorithm. Previous attempts to improve on HCR, such as the Greediest Heaviest Observed Sub-Tree (GHOST), include discounted weight for orphaned

blocks. PoEM leverages entropy calculations to improve the consensus mechanism. This method computes the change in entropy for each block, using intrinsic difficulty to minimize latency-driven forks and enhance the efficiency of the chain's hash function.

PoEM uniquely enables hierarchical coordination of sharded blockchains. PoEM with workshares is in Nash equilibrium, unlike vanilla Proof-of-Work, thus eliminating selfish-mining. The process of achieving consensus using PoEM is deterministic, ensuring that all data within the network resolves to the same canonical head. This innovative approach also shifts the consensus mechanism's focus from multi-round consensus to single-shot communication. PoEM has shown a 28.5% improvement in confirmation delay and a 16.3% improvement in throughput in a single chain setting. However, PoEM dramatically outperforms all current systems by enabling a chain with many shards.



HORIZONTAL SHARDING

Horizontal sharding is the premise that a blockchain's state and history can be split into multiple partitions in order to increase capacity. These partitions are interoperable through cross-shard transactions. This allows transactions to transfer state trustlessly between shards and create composable intershard contracts. The goal of horizontal sharding is to lower fees for users while retaining network-wide security that approaches a non-sharded system.

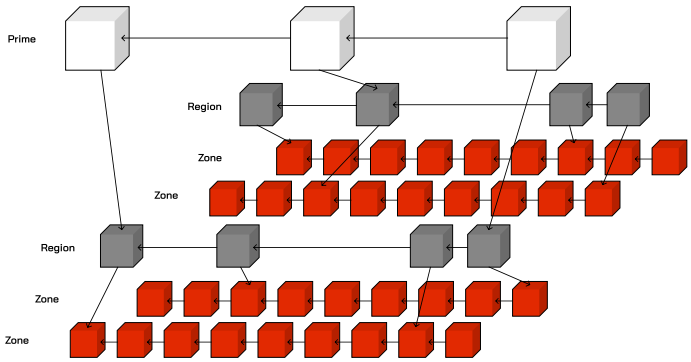
The horizontal sharding design for Quai network is composed of a set of interlinked merge-mined chains - organized into a three-tier hierarchy - that operate efficiently as a single, homogenous layer with shared security. The three layers of the hierarchy are defined as:

- **Prime:** The "root" layer of the hierarchy
- **Region:** Secondary coordination layers
- **Zone:** Layer where transactions take place

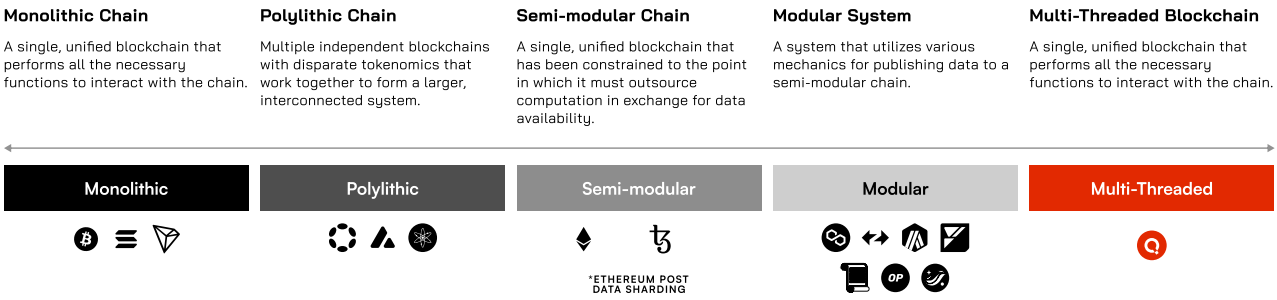
WHAT IS MERGE-MINING?

Merge mining is when a miner is able to create valid blocks for two separate blockchains. In practice, this allows a single computer to mine and secure many blockchains simultaneously with no increase in hardware requirements or energy consumption.

In the context of Quai Network, merge-mining enables what is called a "coincident block". In academic circles this might be referred to as a superblock. However, in Quai a coincident block is not just for compressed referencing, but also creates valid blocks in multiple chains allowing for objective cross-chain linking. Coincident blocks occur when a Zone block has reached a difficulty threshold that is valid in a higher context (i.e Region or Prime). Therefore when a coincident block is found, it is simultaneously a Prime, Region, and Zone block. Coincident blocks are the cornerstone of the cross-shard communication protocol used in Quai Network by creating shared reference points up and down the hierarchy. This ensures atomicity in cross-shard execution as shards are "interwoven" together.



This design allows for the decoupling of local and global data consistency & state consensus functions, and parallel processing of transaction and contract interactions, within separate shards across the network.

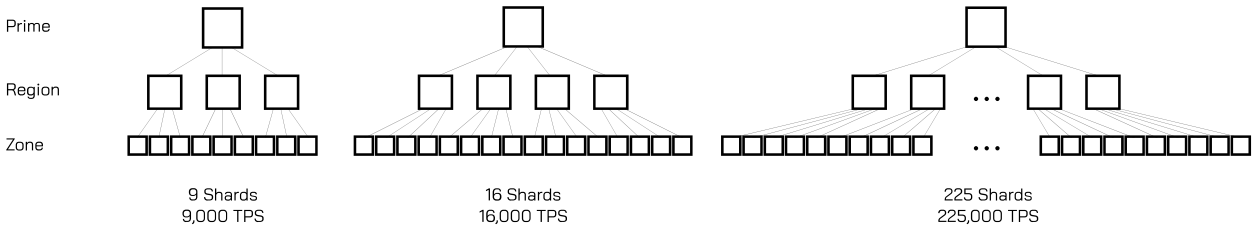


Finally, it is interesting to note that any technique for scaling that is used in a monolithic, semi-modular, or modular architecture can be applied on top of the multi-threaded approach. Therefore, if any competing system can increase throughput in a single chain, those improvements can easily be implemented for all of the Zone chains in the sharded architecture.

Quai Network separates the execution of transactions and state based on address space. This allows nodes and wallets to quickly identify which shard an address resides on by looking at the first byte. For example, all addresses starting 0x00 are in shard 1 while all addresses starting with 0x01 are in shard 2.

Quai Network begins with a single shard and dynamically adds new shards as network demand increases. Adding more shards into the hierarchy enables higher throughput, at the cost of increased cross-chain settlement

times. Therefore, it is desirable for the network to activate only as few shards as are necessary to satisfy the users' demand. The protocol itself handles this, basing decisions on the required number of shards by measuring the rate of uncle blocks.

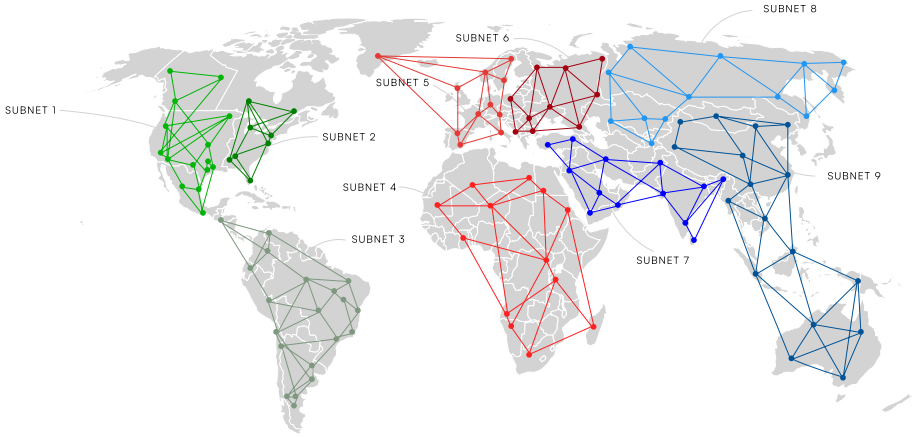


Expected Max TPS	# of Zones in each Region	Total Number of Shards	Mean Cross-Region Settlement Time	Mean Cross-Prime Settlement Time	# of Regions in Prime
1,000	1	1	N/A	N/A	1
2,000	2	2	20s	N/A	1
4,000	2	4	10s	20s	2
9,000	3	9	15s	45s	3
-	-	-	-	-	-
256,000	16	256	80s	1280s	16

It is important to note, that while mean cross-Prime settlement time can reach up to 600 seconds at 50,000 TPS, this is still orders of magnitude shorter than Visa's 180 day settlement and fraud-proof Layer-2 settlement of 7 days.

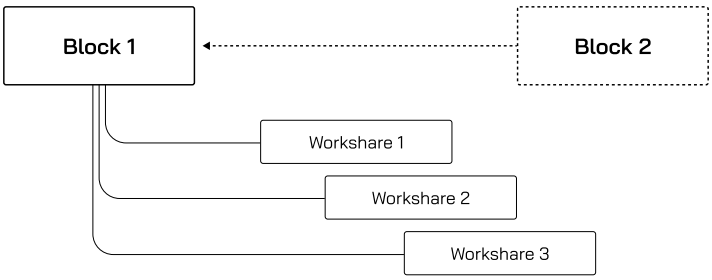
SELF-ORGANIZED SUBNETS

Geographic grouping within self-organized subnets further enhances network performance by reducing latency and optimizing bandwidth usage. Nodes are incentivized to group into optimized network topologies, allowing transactions to be propagated more efficiently within each geographic region. For example, the bandwidth overhead in traditional peer-to-peer networks can be as high as 10-100x the data included in a block, but with Self-organized Subnets, this is significantly reduced.



WORKSHARES

Workshares in Quai Network are a pioneering approach to achieving finality based on cumulative economic effort, enhancing both security and efficiency. Traditionally, finality in Proof-of-Work blockchains has been determined by chain depth, with blocks being the primary mechanism to sample the hashrate. Workshares, however, represent subsamples of hashrate proposed by miners as they search for the next block. When a miner reaches a lower threshold than what is required for a block, they propagate a workshare to peers, signaling the reference point of the prior block.



Additionally, workshares are utilized to propagate groups of transactions through the network in a DDOS tolerant way. By referencing transactions in the workshares, transactions can efficiently propagate as groups rather than singletons, dramatically reducing the overhead of managing requests as well as decreasing the amount of bandwidth wasted in replication. This proactive distribution makes it likely that most nodes will have already received transactions prior to them being included in blocks. This allows nodes to pre-process some validations, such as signatures, as well as enabling the use of block transaction manifests.

Moreover, workshares effectively build a distributed mining pool into the base protocol. This allows miners to get paid 20-50x as often as they would without workshares. By increasing the frequency of payments to miners, there is a smaller incentive to mine in a pool as the issue of infrequent payouts is minimized.

Additionally, by paying for work shares rather than paying for blocks, Quai creates two previously unrealized game theoretic outcomes. Firstly, miners now have an incentive to propagate transactions. Secondly, the concept of withholding blocks due to ex-protocol ordering incentives is eliminated. This is one of the key pieces that allows PoEM to achieve a Nash equilibrium where PoW was unable.

STATE RENT

As blockchain usage grows, maintaining account state becomes increasingly complex and costly. State rent addresses this by introducing a cost for the state used by an account in the state tree, ensuring sustainable network performance. By pricing account slots logarithmically according to the size of the account trie, the market can dynamically determine the price through buying and selling account space. This ensures that costs borne by the entire network are paid by the transactor. This creates a long-term sustainable state market which reflects the costs associated with increased state.

The approach utilized in Quai Network leverages market dynamics to set prices for account slots, reflecting the varying hardware constraints and preferences of node operators. Accounts must pay for their index in the Patricia Merkle Trie (PMT), and they can sell back their space when no longer needed. This system not only incentivizes users to manage state usage efficiently but also introduces a feedback mechanism to prevent resource overconsumption and speculative exploitation. By setting account slot prices based on trie size, the state rent balances resource usage, encourages efficient state management, and allows the network to scale as needed.

INTRASHARD PARALLEL TRANSACTION PROCESSING

Quai Network introduces parallel transaction processing system that significantly boosts throughput and efficiency by enforcing access lists. Unlike traditional EVM-equivalent systems limited by sequential processing, Quai Network parallelizes transactions within shards. By breaking down transaction structures and managing

dependencies through access lists, the network handles processing multiple transactions concurrently, reducing block processing times and increasing capacity.

Key Features:

1. **Enforced Access Lists:** Each transaction explicitly defines which accounts and storage slots it can access. This pre-declaration allows the system to identify non-overlapping transactions that can be safely executed in parallel.
2. **Dependency Management:** By analyzing the access lists, the network can construct a dependency graph for transactions, allowing it to maximize parallelization while avoiding conflicts.
3. **Concurrent Execution:** Non-conflicting transactions within a shard are processed simultaneously, reducing latency and increasing capacity.

This approach leverages the fact that over 80% of historical EVM transactions have non-overlapping dependencies. By explicitly defining which accounts and storage slots transactions can access, Quai Network minimizes conflicts and enables efficient parallel execution.

SHARDED CLIENTS (GLOBAL VS. SLICE)

The Quai Network client is configured to allow nodes to run various subsets of shards. This means when running a node, users have the choice of selecting:

1. **Global Node:** A global node on Quai Network maintains the ledger and generates proposed blocks for mining in all shards. Running a global node ensures proper cross-shard execution for all transactions. Global nodes have the highest resource requirements at roughly 8 CPU, 32GB of RAM, and 1TB drive.
2. **Slice Node:** A slice validates prime, a single region, and a single zone. The benefit to running a slice node is that a node needs fewer resources. The slice node requires 4 CPU, 8GB RAM, and 1TB drive.
3. **Multi-Slice Node:** A multi-slice node is the configuration between a slice and a full global node. Node runners may opt to run a multi-slice node if their machine is larger than the requirements for a slice node but not enough for a global node

NIPOPOWS

The Quai Network leverages Non-Interactive Proofs of Proof-of-Work (NiPoPoWs) to allow applications to verify the state of the blockchain without needing to download the entire blockchain history, run a node, or trust a centralized indexer. This is achieved by using succinct proofs that are logarithmic in size relative to the blockchain.

By integrating NiPoPoWs, Quai Network supports RPC proving in the quais.js SDK, facilitating trustless interactions within the network. This allows data consumers to become agnostic of data providers. Thus, NiPoPows will eliminate the need for centralized trusted indexers, while also allowing the applications built on the network to use all running nodes to scale. Moreover, decentralized data providing will create a new revenue stream for node operators which previously did not exist.

DUAL-LEDGER

As noted in subsequent sections, the system has two native coins - Quai and Qi. Quai is an EVM compatible account ledger. Qi is a fixed denomination UTXO ledger.

Despite its intended use as a form of digital cash, Bitcoin and other UTXO-based ledgers face limitations in fungibility and other aspects, hindering widespread adoption as a cash equivalent.

The UTXO ledger addresses these limitations by utilizing fixed denominations, thereby enhancing the fungibility of its native asset, Qi. This design mirrors the characteristics of traditional cash, with Qi denominations resembling quarters, dimes, pennies, and bills. The standardized denominations are as follows:

DENOMINATION	NUMBER OF QI
0	0.001 Qi
1	0.005 Qi
2	0.01 Qi
3	0.05 Qi
4	0.1 Qi
5	0.25 Qi
6	0.5 Qi
7	1 Qi
8	5 Qi
9	10 Qi
10	20 Qi
11	50 Qi
12	100 Qi
13	1000 Qi
14	10000 Qi
15	100000 Qi
16	1000000 Qi

Additionally, the UTXO ledger in Quai Network is designed to be purely transactional, as it does not support any form of scripting. This restriction further enhances the fungibility of Qi and underscores its primary focus on facilitating payments.

ETXS

External Transactions (ETXs) are the mechanism used to transfer state between two Quai shards. These transactions are communicated via hash-linked references created by coincident blocks, which ensures atomic cross-shard state transitions. To support contract-based ETXs, two new opcodes have been integrated into the Ethereum Virtual Machine (EVM). These opcodes enable cross-shard smart contract composability.

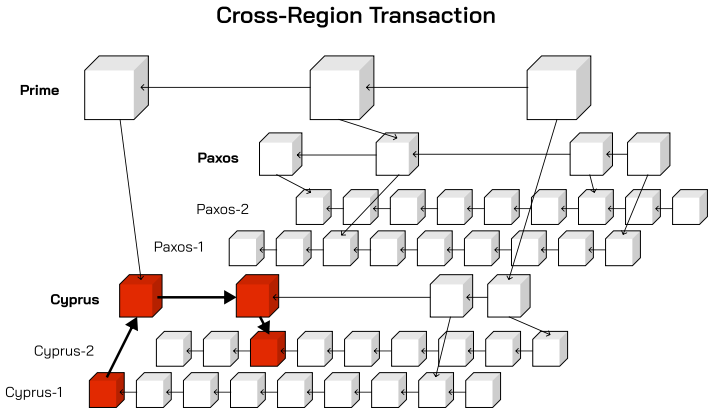
ISADDRINTERNAL: Checks if an address is tied to that shard

OP_ETX: Emits the cross chain data

ETXs navigate through the hierarchical structure of the Quai network, always passing through a dominant chain—either a Region chain or the Prime chain. The following diagrams gives examples of trustless state traversal within the network:

Origin Chain: The blockchain from which the ETX is initially broadcast.

Destination Chain: The blockchain to which the ETX is sent.



For an ETX to reach its destination, it must first ascend the hierarchy from the origin chain to a dominant chain associated with the destination chain. Subsequently, it descends the hierarchy into the subordinate destination chain. ETXs are categorized into two types: account-initiated and contract-initiated.

To facilitate the propagation of ETXs, two data fields (manifest & etxRollup) are included in the headers of all Quai blocks. These fields enable ETXs to be forward-propagated to coordinate blockchains. Forward propagation significantly reduces the instantaneous bandwidth and processing required to service ETXs, thereby enhancing the efficiency and scalability of the network.

PROGPOW

Quai Network employs Programmatic Proof-of-Work (ProgPoW) as its mining algorithm, which is ASIC resistant and GPU friendly. Unlike ASICs, which are specialized and often lead to centralization due to their high cost and limited availability, GPUs are global commodity hardware that are widely available and used for many applications. This widespread availability ensures accessible mining, preventing the monopolization of mining power by a few entities and enhancing the overall security and resilience of the network.

ProgPoW is specifically designed to leverage the strengths of commodity hardware, optimizing its algorithms to utilize the full capabilities of general-purpose GPUs. This not only democratizes access to mining but also aligns the network's security with a broader user base, fostering a more decentralized ecosystem. By doing so, ProgPoW mitigates the risk of centralization associated with ASIC mining, ensuring that the network remains accessible to a wider range of participants and promoting a more equitable distribution of rewards. This strategic choice underscores Quai Network's commitment to maintaining a robust, decentralized infrastructure that can support scalable and efficient blockchain operations.

EVM

Quai Network integrates the Ethereum Virtual Machine (EVM) into its architecture, leveraging its standardized and robust frameworks to provide a familiar and reliable environment for developers. The EVM, being a well-established and widely adopted standard in the blockchain community, offers extensive support for smart contract development, ensuring compatibility and ease of use for developers transitioning from other platforms. This strategic choice not only accelerates development and deployment processes but also enhances the network's programmability, enabling the creation of sophisticated decentralized applications (dApps) with proven reliability and security.

Quai & Qi Design Mechanisms

The Quai and Qi coins are designed to create a store of value, unit of account and medium of exchange, thus fulfilling the requirements for a monetary system.

Quai is meant to hold and accrue value long-term with network growth, and act as a programmable monetary layer, providing the foundation for financial instruments/markets to be built on top and as part of the same system.

Qi is meant to have stable purchasing power, connected to the cost of energy, and act as a non-fiat dollar alternative that is used as decentralized crypto cash.

QUAI	QI
Traditional digitally scarce crypto asset, with added programmability and accruing value with network growth.	Cryptocurrency designed to enable and scale with adoption and transactional use, connected to the cost of energy.
Constrained supply, with potential growth of new block reward issuance trending asymptotically toward zero.	Accommodative supply with highly reactive issuance/inflation rate in direct proportion to demand.
Account based model with smart contracting capabilities.	UTXO set model with p2p transfers and no scripting.

KEY MECHANICS OVERVIEW

- ▶ The following mechanics govern all post-genesis coin supply and issuance (there is a pre-set initial allotment of Quai supply generated and allocated as part of the genesis block).
- ▶ Quai and Qi coins are minted by the same work-based PoEM consensus process that secures the network,

and are paid to miners in the form of block rewards..

▷ Both coins are designed with a dynamic issuance model for responsive block rewards based on the network mining difficulty. The Qi reward function is linearly proportional to difficulty. The Quai reward function is proportional to the binary logarithm of difficulty.

▷ Continuous difficulty and reward adjustments are conducted on a rolling basis. This results in the quantities and ratio of Quai and Qi rewards changing with each new block.

▷ Miners elect to receive either Quai or Qi as a block reward. They can change their selection on each block. Thus, they are competitive substitutes for new reward issuance supply, ie, mining Qi reduces potential Quai emission and supply (and similarly in the reverse direction).

▷ Miners may also choose to lock their rewards for a longer duration to receive a multiplier on the quantity of Quai or Qi coins they ultimately receive.

▶ Additionally, a fully automated two-way conversion mechanism is built into the protocol. This enables all users to convert Quai to Qi or Qi to Quai at the current protocol exchange rate. When conversions take place the protocol burns the input token and mints the output token.

There is no fixed peg, backing nor collateralization, between or underlying either the Quai or Qi coins.

BLOCK REWARD FUNCTIONS

Quai and Qi block reward emissions are both calculated as functions of a measure of difficulty – or how hard it is to mine a block – but use exponentially different forms, with Quai rewards in logarithmic proportion and Qi rewards in linear proportion.

Quai rewards are issued in proportion to the "bits" of difficulty, approximately represented by the number of leading zeros in the target value, which is also logarithmically proportional to the hashes of difficulty measure used by Qi. As such, the percentage growth of Quai supply trends asymptotically toward zero overtime.

Qi rewards are issued in direct proportion to "hashes" of difficulty, tied to the hashrate, or more specifically to the expected number of hashes needed to mine a block at the current difficulty target. Supply is inflationary at a higher or lower rate depending on market demand.

The block reward functions are as follows:

$$\text{BlockReward}_{QUAI} = k_{QUAI} * \log_2 (\text{Difficulty})$$

$$\text{BlockReward}_{QI} = k_{QI} * \text{Difficulty}$$

Where:

Difficulty is the expected number of hashes needed to mine a block at the current difficulty target value.

k_{QUAI} is the variable that converts the scale of the difficulty measure into an appropriate magnitude for the actual number of Quai tokens offered in the block reward and, more importantly, is the mechanism by which the ratio of Quai:Qi rewards are updated on an ongoing basis as part of the adjustment process via a controller mechanism. The objective of this controller, and its resultant effect on the k_{QUAI} variable, is to push the system back toward an equilibrium, defined as when the market value of the block reward in Quai tokens is equal to the market value of the block reward in Qi tokens, and both are equal to the cost of mining a block (such that miners are economically indifferent as to whether they select/receive their reward in either Quai or Qi, and expected to continuously maintain devoted hashpower in line with actual/expected network token demand).

k_{QI} is the variable that converts the scale of the difficulty measure into an appropriate magnitude for the actual number of Qi tokens offered in the block reward. It also has a decaying component to account for the projected growth in processing power over time, so that the Qi block rewards more closely reflect the energy cost of mining, rather than the increasing efficiency of computing power.

Exact function values for K_{QUAI} and K_{QI} will be publicly finalized prior to mainnet.

The above block reward functions only define how many Quai or Qi can potentially be emitted. Actual, realized new supply emissions from block rewards are determined by the choices miners must make to receive only either Quai or Qi, a selection they may change on a go-forward basis at any time.

OPTIONAL REWARD LOCK & MULTIPLIER

Just as miners may choose to receive either the Quai or Qi block rewards, they may also choose whether: (i) to receive those Quai or Qi block reward coin amounts as they normally would when they successfully mine a block; or, (ii) to receive some greater multiple of that coin amount in a time-locked format, only useable/spendable at some point in the future. Miners may also change their selection at any time (just as they can between choosing Quai or Qi rewards).

The durations and multiples of the available lock options will be finalized before mainnet launch, and for illustrative purposes, might look like something like: (i) receive 1x coins normally upon successfully mining a block; (ii) receive 1.035x coins with a 3-month lock; (iii) receive 1.1x coins with a 6-month lock; or, (iv) receive 1.25x coins with a 12-month lock. The multiples on various lock durations will degrade over time (and then settle at levels that continue in perpetuity or may eventually go away entirely). For example, the initial multiples may be available for one year and then be halved in each subsequent year until year five, and then continue at those year five levels in perpetuity, as illustrated in the table below.

Lock Duration	BLOCK REWARD TOKEN MULTIPLES*				
	Year 1	Year 2	Year 3	Year 4	Year 5+
2 weeks[1]	1.000000	1.000000	1.000000	1.000000	1.000000
3 months	1.035000	1.017500	1.008750	1.004375	1.002188
6 months	1.100000	1.050000	1.025000	1.012500	1.006250
12 months	1.250000	1.125000	1.062500	1.031250	1.015625

In addition to its impact on token emissions/supply, this feature also serves a real, functional purpose and benefits the network:

> All proof of work coins have some duration or lock-up on the coins, but without a multiplier. For example, even in Bitcoin, a miner reward has a block maturation time such that its coins cannot be spent for some period of time, though there is no multiplier concept. This duration lag/lock provides a buffer for the ongoing consensus process to play out in a more predictable manner and ensure no double spending of rewards in the event of short term, small re-orgs at the tip of the chain. Increasing this lag/lock time provides even further certainty around the consensus process and avoiding double spending of rewards.
>
> The introduction of a multiplier for block rewards serves to increase and further ensure chain security.

1 Miner rewards are spendable after a cooldown lock period of ~ two weeks, a similar mechanic as found in other PoW systems (eg in Bitcoin, coinbase transactions are only spendable after 100 blocks).

* Block reward token multiples are subject to change prior to Mainnet

Most simply, it creates greater possible incentives for miners who secure the chain, eg, it increases the coins offered in block rewards to miners in a sustainable, long term way. It also adds disincentives to the possibility of miners acting adversarially or adversely attacking the chain (or being bribed or co-opted to do so), by creating sunk costs that miners stand to lose in much the same way that ASIC hardware requirements do for Bitcoin and many other PoW networks.

Quai uses an ASIC-resistant algorithm to allow mining with GPU hardware that is not specific to the network but repurposable for other uses. This provides greater mining access, less centralized hashrate distribution, and a more elastic hash power market. However, because GPU hardware can be repurposed and is thus still valuable outside of the network, it lacks some sunk cost disincentives against network attacks/threats that ASICs provide. That is, because ASICs can only be used for mining the network, any act to attack/devalue the network also similarly destroys the value of the ASIC hardware - which can be viewed as a sort of up-front locked-in capital commitment by miners.

Thus, the addition of miner block reward multipliers re-introduces the same underlying concept as ASIC mining hardware does, serving as a sort of standing capital commitment, the value of which is tied to the value of the network. That is, miners who elect to lock up their block rewards for some duration will be less likely to attack or act adversely to the network since any destruction/reduction in network value will also destroy/reduce the value of these block rewards they're set to receive in the future.

The team will release the exact durations and multiples of the available lock options before mainnet launch.

NATIVE QUAI/QI TOKEN CONVERSIONS

As initially noted in the key mechanics overview, a fully automated conversion mechanism built into the protocol enables all users to provide/burn existing Qi or Quai and mint/receive new Quai or Qi at the current block reward ratio, at any time.[2] That is, if the current potential block reward amount is x Quai coins and y Qi coins, conversions can be done at an exchange rate of x:y.

2 Just as for miner block rewards, there is a cooldown lock period of ~ two weeks on the new coins received through the native protocol conversion mechanism.

DIFFICULTY AND REWARD ADJUSTMENTS

At the top level, the Quai network works similar to most other work-based systems, determining block production intervals and thus emissions rates, by setting block rewards and adjusting difficulty level/target.

While systems such as Bitcoin implement difficulty adjustments at the end of sequential periods (~ 14 days or 2016 blocks, given its 10 minute target block time interval) and update block rewards over longer-term epochs (~ 4 years), Quai does so for both continuously on a per block basis, using a rolling look-back across a previous period (360 blocks or ~ 72 minutes, given its 5 second target block time interval).

This means that the difficulty, as well as the respective and relative quantities of Quai and Qi block rewards, change - up or down - with each new block.

Difficulty is adjusted in response to miner hashrate changes to cause observed block times to approach the target time. For example, if blocks are produced faster than the expected/target block interval time (which occurs due to increased hashrate), then difficulty must be adjusted upward to return to the target block interval time. Similarly, if blocks are produced more slowly, then difficulty is adjusted downward.

The new difficulty measure for each new block is used for both Quai and Qi block rewards functions. Additionally, the resultant Quai and Qi block rewards, and the ratio between them, are adjusted with each new block based on the k_{QUAI} and k_{QI} factors of the block reward functions described above.

k_{QI} is simply a conversion constant along with a predefined schedule of decay intended to account for the projected growth in mining efficiency or processing power, calculable according to the current block and network difficulty.

k_{QUAI} is adjusted via a controller optimizing back toward its defined equilibrium where the market preference for Quai and Qi is neutral at the protocol defined rate. Tactically, this means that when there is more Quai selected by miners as block rewards and minted via conversion, the market value of the block reward in Quai is greater than that in Qi, and as such k_{QUAI} must be adjusted upward such that there will be fewer Quai coins per block (remember that k_{QUAI} is part of a negative exponent within the Quai block reward function).

Conclusion

Quai Network represents a fundamental reimagining of blockchain infrastructure, designed from the ground up to overcome these limitations and fully realize the original vision of cryptocurrency. By taking an integrated approach and incorporating key innovations at the base layer, Quai creates a foundation capable of supporting the complex, high-speed, and high-stakes transactions that will define the future of global finance.

Quai's architecture, featuring PoEM consensus, horizontal sharding, and self-organized subnets, enables unprecedented scalability without sacrificing security or decentralization. The dual-coin system of Quai and Qi provides a novel approach to digital currency, offering both a store of value and a stable medium of exchange intrinsically linked to energy expenditure.

By combining advanced blockchain technology with a forward-looking economic model, Quai creates a platform capable of supporting a wide range of applications, from everyday transactions to complex financial instruments and decentralized systems. It's not just a new blockchain or cryptocurrency; it's a fundamental building block for the economy of the future.

As we stand on the brink of this new economic era, Quai offers the potential to revolutionize value exchange, and economic organization on a global scale. It provides the infrastructure needed to truly deliver on the original promise of cryptocurrency: a decentralized, accessible, and efficient system for transferring and storing value in the digital age.

Glossary

POEM (PROOF OF ENTROPY MINIMA): The consensus mechanism used by Quai Network that incorporates intrinsic block weight to reduce orphan rates and accelerate finalization.

HORIZONTAL SHARDING: A technique to split blockchain state and history into multiple partitions to increase capacity.

WORKSHARES: Subsamples of hashrate proposed by miners as they search for the next block, used to improve transaction propagation and network efficiency.

ETXS (EXTERNAL TRANSACTIONS): A mechanism to facilitate trustless transfer of state between two Quai shards.

PROGPOW (PROGRAMMATIC PROOF-OF-WORK): A mining algorithm designed to close the efficiency gap between GPUs and ASICs.

NIPOPOWS (NON-INTERACTIVE PROOFS OF PROOF-OF-WORK): A method allowing lightweight clients to verify the state of the blockchain without downloading the entire history.

UTXO (UNSPENT TRANSACTION OUTPUT): A model of tracking ownership of cryptocurrency where each transaction consumes previous outputs and creates new ones.

EVM (ETHEREUM VIRTUAL MACHINE): A computation engine used by Quai Network for executing smart contracts.

QUAI: The primary network token of the Quai Network, designed to be more scarce over time.

QI: The secondary token of the Quai Network, designed to reflect value connected to the cost of energy.

COINCIDENT BLOCKS: Blocks that are valid across multiple levels of the Quai Network hierarchy simultaneously.

STATE RENT: A mechanism to price account slots based on their impact on the state tree.

SELF-ORGANIZED SUBNETS: Geographic grouping of nodes to optimize network performance and reduce latency.

BLOCK REWARD FUNCTIONS: Mathematical formulas determining the issuance of Quai and Qi tokens as mining rewards.

K_{QUAI} AND K_{QI}: Factors in the block reward functions that influence token issuance rates.

DIFFICULTY: A measure of how hard it is to mine a block, typically expressed as the expected number of

hashes needed.

GENESIS ALLOCATION: The initial distribution of tokens at the launch of the network.

MERGED MINING: The process of mining multiple cryptocurrencies simultaneously without requiring additional proof-of-work.

GLOBAL NODE: A node that maintains the ledger and generates proposed blocks for all shards in the Quai Network.

SLICE NODE: A node that validates only a subset of the Quai Network shards.

FURTHER READING & REFERENCES

Website: https://qu.ai

Docs: https://qu.ai/docs

Discord: https://discord.gg/quai

Twitter/X: https://x.com/QuaiNetwork

Github: https://github.com/dominant-strategies

PoEM paper 1 https://arxiv.org/abs/2303.04305

PoEM paper 2 https://eprint.iacr.org/2024/200.pdf

BlockReduce paper https://arxiv.org/pdf/1811.00125

LEGAL DISCLOSURE

This document is for informational purposes only and is not intended to be a solicitation or offer to buy or sell any securities or related financial instruments. The information contained herein has been obtained from sources believed to be reliable but is not necessarily complete and its accuracy cannot be guaranteed. No representation or warranty, express or implied, is made regarding the accuracy or completeness of this information, and it should not be relied upon as such.

Any opinions expressed herein are subject to change without notice. Quai and its affiliates, and employees do not accept any liability whatsoever for any direct or consequential loss arising from any use of this document or its contents. This document may contain forward-looking statements, which reflect our current views with respect to, among other things, the operations and technical performance of our ecosystem. You should not place undue reliance on these forward-looking statements, which apply only as of the date of this document.

The information provided in this document is provided “as is” without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. The contents of this document could be outdated, and we make no commitment to update such materials. We assume no responsibility for errors or omissions in the contents of this service.

The contents of this document do not constitute advice and should not be relied upon in making or refraining from making any decision. All material contained within this document is subject to change without notice. Recipients of this document are expected to respect the confidentiality of the information contained herein and refrain from copying, distributing, or disclosing it to third parties without the express written permission of our company.

The information contained herein may be subject to legal restrictions or liabilities on the dissemination of information and must be treated accordingly.

Contact Information: support@quai.org