Koinos: A free-to-use dApp platform with a provably egalitarian, fast, and fee-less digital currency

Koinos Group
contact@koinos.group
koinos.io

Abstract

A general purpose blockchain-based decentralized network that allows for free-to-use applications through a “Mana” mechanism that dynamically prices network resources in opportunity cost (not tokens) and allows for free-to-use dApps through Mana “delegation.” Proof-of-burn is implemented as a consensus algorithm to maximize efficiency, decentralization, and provable egalitarianism while thwarting the exchange attack and mitigating spam. Blocks are produced by hashing a private key and the random number output of a verifiable random function (VRF) then dividing by the amount of tokens burned. Like proof-of-work, the longest chain serves as an immutable record of transactions backed by the largest pool of sacrificed capital. The Koinos blockchain framework is used for fork-less upgrades as a result of its modular upgradeability. This creates a free-to-use and truly decentralized general purpose blockchain with a mainstream user experience that maximizes accessibility to end-users, developers, and node operators.

Previous Work

Satoshi Nakamoto created the first decentralized peer-to-peer digital currency in Bitcoin by designing a novel database architecture (the blockchain) that leveraged fees to regulate network usage and proof-of-work to regulate state transitions. Ethereum retained these primitives and the blockchain database but created more general utility by allowing users to include Turing complete code in their transactions. That code would then be executed in a virtual machine, thereby allowing for decentralized applications (dApps).

Prior to developing Koinos we were the core developers of Steem (the first fee-less and social blockchain) up until a hostile takeover and exchange attack. After leaving that project, our goal was to build a company that would empower developers to build dApps like Steem and Hive, but on a truly decentralized and fee-less blockchain that would resist the exchange attack. Unfortunately, none of the existing blockchains had the properties we needed. The "fee-less" blockchains were not truly fee-less, requiring that users pay for RAM and/or accounts nor were they truly decentralized as a result of their launch (ICOs) or their consensus algorithm, and often both.

We wanted to take blockchain accessibility to the extreme by enabling, for the first time, *free-to-use* dApps which would require not only fee-less transactions, but free accounts, free smart contract execution, and network resource delegation. Delivering these capabilities required building an entirely new blockchain from the ground up and executing a provably fair decentralized launch. The end result would be a general purpose blockchain that was not just another Ethereum competitor, but the first genuine alternative to Ethereum.

$KOIN

Prior to KOIN, most cryptocurrencies had relatively simple token economic designs; they were the token used to pay the fees necessary to sustain the operations of the decentralized network. Counterintuitively, removing the fees is what allows for the creation of a more dynamic, flexible and performant system which supports a digital currency that finally delivers on the futuristic vision of an egalitarian and decentralized digital currency that began with Bitcoin.

Token Supply & Distribution

To maximize decentralization and provable fairness from the very beginning, the KOIN token was launched in the same manner as Bitcoin; through proof-of-work mining (on Ethereum). The max supply of mineable tokens was 100 million KOIN. When Koinos mainnet goes live, token balances will be initialized using a snapshot of the KOIN ERC-20 and the initial target rate of new token creation will be 2%, but this can be altered in-band by governance (see the Fork-Less Upgradeability and Decentralized Governance sections). The burn component of the consensus algorithm could result in a much lower actual inflation rate and even temporary periods of deflation.

As a result of the novel “Mana” system (see the Mana section) the mainnet tokens can be transferred without paying any fee because the Mana contained within them allows the holder to use the network without spending any KOIN. The Mana system makes Koinos the first truly free-to-use blockchain as users do not have to purchase accounts, pay to execute smart contracts, *or even acquire KOIN tokens* in order to use the blockchain.

Inflationary & Deflationary

As the first general purpose blockchain to implement proof-of-burn as a consensus algorithm, the KOIN token supply will expand and contract based on market conditions, thereby delivering the kind of economic “levers” featured in the most advanced global currencies, but administered in a fully decentralized and algorithmic manner (see the proof-of-burn section).

Fast & Free

Since proof-of-burn eliminates the need for meaningless computational work, Koinos blocks can be produced rapidly allowing the KOIN token to be both fee-less *and fast*. The incredible upgradeability of Koinos allows block times to be continually lowered over time, thereby decreasing latency, limited only by network stability and state growth considerations. With these features in place, the KOIN token can empower people to exchange unlimited value in seconds without losing anything to a fee, thereby opening up entirely new—and currently unimaginable—business models to entrepreneurs and developers.

Fork-Less Upgradeability

When developing Steem we saw firsthand how hard forks are holding back blockchain adoption by creating a major bottleneck in the upgrade process. Mainnet solves this problem through its use of the Koinos blockchain framework which allows any behavior to be added to the blockchain as a smart contract. The fundamental assumption of this framework is that any smart contract can be upgraded by an authorized party. In the case of system logic, the system governance contract has the authority to make a “user smart contract” into a “system smart contract” in-band (no hard fork) that overrides some basic, native implementation. In this way, upgrades to the blockchain’s business logic can be pushed to the p2p network much like an operating system patch with minimal network disruption.

The Koinos blockchain framework is effectively the world's simplest, fully functional, general purpose blockchain contained within a microservice architecture. The blockchain (i.e. the chain microservice) features natively implemented system calls that contain only the cryptographic functions necessary for constructing a technically true blockchain along with logic for dispatching a node between the native system calls and newer system calls implemented as smart contracts (i.e. WASM implementations) running in the virtual machine. This combination of native implementations and "system smart contracts" form a high-performance, vertically scalable, and upgradeable blockchain "kernel" (the framework) that allows for any behavior to be added to the blockchain without requiring a hard fork.

Universal Language Support

Ethereum dramatically expanded the creative space available to developers by allowing them to leverage a single, custom-built, Turing complete programming language; Solidity. Koinos dramatically expands that creative space once again by allowing developers to work in *all* of the most used Turing complete programming languages, starting with C++ and TypeScript (using AssemblyScript), but with more languages to come. Koinos accomplishes this through the combination of three open source technologies built and maintained by the best teams in the world, all of which have ever-increasing language support. They are: (1) WebAssembly, (2) Protocol Buffers, and (3) the Advanced Message Queuing Protocol.

WebAssembly is used for smart contracts. Protobuf is used for serialization within the node, and AMQP manages communications between microservices which utilize broadcast messages to implement an event-driven paradigm. These technologies make it far easier to implement an SDK for any programming language that all three support; which is practically all of the most used Turing complete programming languages.

Mana

Our goal with Koinos is to support decentralized ("Web3") applications that have a Web2 user experience. In short, dApps must have a delightful user experience and people must be able to begin using them without first having to acquire tokens which is a major barrier to entry. The Mana system is how we accomplish those objectives.

We call it “Mana” because the user experience replicates that of the RPG video games so many people are already familiar with.

The basic premise of the Mana system is that every KOIN token is “born” with 1 Mana which can be consumed when a user consumes network resources. Mana is a property of the KOIN token, it is not a token itself. It therefore cannot be bought or sold and cannot acquire its own price distinct from the KOIN token. Users can, however, delegate their Mana to other users, thereby allowing non-token holders to begin using the blockchain while still effectively mitigating spam. That Mana is still tethered to the delegator’s KOIN to ensure the economic sustainability of the system and maximize liquidity for the delegator who can undelegate at-will.

Implementation Details

Like Ethereum’s gas, every VM instruction will have a specific cost in Mana. Since only a limited amount of instructions can be included in a block, Mana is tightly coupled to the network resources available to users. Whereas Ethereum requires the user to purchase gas from miners which then gets consumed by the transaction, the Mana system autonomously consumes the appropriate amount of Mana from a user’s balance based on the resources consumed by their transaction.

“Paying” in Time

Once any of the Mana in a given token is consumed, that token is locked for 5 days, so they can develop a weekly “rhythm”to their blockchain (and dApp) usage. This creates an opportunity cost in lieu of a real-time monetary cost that serves to disincentivize the submission of value-less transactions. This fixed period of time functions as a “regen time” which creates the user experience of Mana “regenerating over time,” creating a fun, almost game-like user experience.

The regen time is based on how long it takes for one satoshi of Mana to regenerate, with regeneration happening on all of a user’s tokens at the same time. Since this mechanism is distributive, the regen time appears dynamic to the user. In other words, a user’s Mana will constantly be regenerating so they will not have to wait the full 5 days to resume their blockchain usage.

Free-to-Use

To solve the problem of allowing people to use dApps without first having to acquire *any tokens whatsoever*, Koinos allows smart contract developers to specify who will

“pay” the Mana when the smart contract is run (“Payer/Payee Semantics”). Each transaction must explicitly specify an address of a payer for the transaction, and optionally a payee. The payer’s Mana is spent and the payee’s account nonce is updated. If there is no payee set, the payer is used for both. The combination of these features allows a smart contract to specify a payer for its Mana costs.

These deceptively simple semantics will not only allow people to begin using the blockchain without having to buy any KOIN, they also give large KOIN holders a powerful tool for supporting valuable dApps without sacrificing any of their tokens.

Multi-Dimensionality

As Vitalik Buterin has explained, Ethereum’s gas calculations are one dimensional, pricing very different resources (e.g. storage and compute) as if they are the same, which is inefficient. With the Mana resource model, the resources are tracked separately to maximize efficiency, but the user is still only charged in Mana. Resources are pooled every block, with a limit to how many of those resources can be consumed per block and an XYK market maker is used to set a price for each of the resources in a given block.

This multi-dimensionality allows developers to optimize their contracts to target underutilized network resources. End-users will prefer those dApps which perform such optimizations because they will get more “bang for their Mana,” creating a positive feedback loop of decentralized self-regulation. This system would gradually and continuously charge users more Mana as they consume more contentious resources and less Mana for consuming underutilized resources. The end result is a simple, efficient, and dynamic system for determining resource costs based on user behavior that guarantees the lowest possible cost, while ensuring that the network is protected.

The Mana charged is simply the linear combination of each resource and cost (e.g. `bandwidth_cost * bandwidth_used + storage_cost * storage_used + compute_cost * compute_used`).

Proof-of-Burn

In addition to being fast with zero fees, the KOIN token is intended to deliver on Satoshi’s original vision of a truly peer-to-peer electronic cash that utilizes spare

computational resources and does not require dedicated hardware. In other words, it is *provably egalitarian.* Iain Stewart proposed proof-of-burn in 2012, a year after proof-of-stake was proposed, and we believe this represents the next stage of evolution in consensus algorithms. Proof-of-burn enables us to accomplish provable egalitarianism by delivering the economics of proof-of-work with even higher efficiency than proof-of-stake. The end result of our implementation is a consensus system that should be *more decentralized* than proof-of-work and *more efficient* than proof-of-stake.

The Exchange Attack

Proof-of-burn as a consensus algorithm is remarkably simple and its unique value is easy to understand. Like proof-of-work it requires that the cost of attacking the network be paid "up front." Like proof-of-stake, no actual hardware has to be purchased and run, aside from the hardware required to produce blocks.

Like proof-of-work the exchange attack is thwarted because the block producer has already lost their money, they are simply trying to get it back by maintaining a correct ledger. Any exchange seeking to leverage user funds to influence governance as a result of greed, coercion, or deception (see the Steem/Tron incident) would first have to destroy user funds, which they would never do. This also reduces the need for the complicated slashing conditions required for proof-of-stake implementations because block producers are effectively "pre-slashing" their capital prior to earning block rewards, as with proof-of-work.

Virtual Mining

A user who wants to earn block rewards burns their KOIN, decreasing the total supply of KOIN. The blockchain distributes "virtual hash power" fungible tokens (VHP) to the block producer which can be used to mine a block without needing to run expensive hardware. As the block producer mines blocks, their virtual hash power (VHP) diminishes over time, requiring them to burn more to continue producing. In this way, burning tokens is equivalent to buying mining hardware which degrades over time and the electricity required to perform proof-of-work.

Inflation

VHP is always treated on a 1:1 basis with KOIN. For every unit of KOIN burned a specified account will receive that many units of VHP. When an account with VHP

receives units of KOIN as a block reward, their VHP balance is reduced by that many units. In this way VHP acts as a proxy for KOIN and the total supply of VHP and KOIN can be summed to establish the "virtual token supply" for the purpose of setting a target rate of new token creation. To ensure that there is always incentive to produce blocks there must be a net positive rate of new token creation. Initially, the target rate of new token creation on mainnet will be 2%.

Deflation

As a result of the burn component, the total token supply can be either increasing (inflation) or decreasing (deflation) depending on the level of competition for block production. If the demand for block rewards is increasing linearly, then at a certain point the rate at which KOIN is being burned will outpace the rate at which new KOIN is being produced. The result would be a decreasing token supply despite the new token creation (i.e. "deflation").

Randomness

Proof-of-burn keeps the core consensus mechanism of proof-of-work, but exchanges energy for time by using a verifiable random function (VRF). Every block will contain quanta (sometimes called "slots"), milliseconds in length, which block producers will compete to produce on. In order to earn back their burn, the block producer must attempt to produce on every quantum. This attempt will involve the block producer using their private key, a timestamp, and the previous random output of the VRF to generate a hash which is then divided by their VHP (i.e. their burn). If the hash is low enough, then they produce (similar to proof-of-work), otherwise they have to try again on the next quantum.

Efficiency & Consistency

The block producer's incentive is not to perform as much work as possible, but to perform *as little work* as is necessary to attempt to produce on every quantum. From here, proof-of-burn behaves the same as proof-of-work except that the block producer only has to hash once per quantum. Because block producers are competing to produce on one of the many quantum inside a block, the end result is continuous block production.

Dividing the hash by the size of the producer's burn guarantees that the dominant factor in selecting a block producer is the size of their burn and not the amount of

computational work they have performed (which will be practically nothing) thereby delivering on the promise of high efficiency.

Mining Pools

Unlike on proof-of-work chains, mining pools on Koinos can *increase* decentralization *and* participation in governance as they could empower non-technical users to allocate their capital to more technical users who can guarantee more uptime and vote in accordance with the desires of their contributors. Users would participate in a mining pool simply by transferring their VHP to another Koinos account which has already been upgraded with a mining contract that autonomously distributes rewards to its contributors.

Increased Liquidity

If at any time the block producer or mining pool participant wants to exit block production, they need only withdraw their VHP from the address and sell it like they would any fungible token. This maximizes liquidity and allows users to exit block production at-will with minimal economic downside.

Centralization Resistant & Provably Egalitarian

With proof-of-burn, there are no mining rigs, just accounts holding VHP tokens, so the rate at which block rewards are paid out is entirely algorithmic. This not only makes it infinitely customizable, but also totally resistant to hardware centralization. All of this makes proof-of-burn the first consensus algorithm to deliver the economics of proof-of-work *and is provably egalitarian*; finally delivering on Satoshi's original vision of a truly peer-to-peer electronic cash that utilizes spare computational resources and does not require dedicated hardware.

Decentralized Governance

The high degree of upgradeability enabled by the Koinos blockchain framework makes governance the bottleneck instead of the hard fork process. Like every system behavior, governance is "just" another smart contract on Koinos, albeit one with system level privileges and special importance in the upgrade process. The governance contract is modeled off of how the Bitcoin network manages upgrades (e.g. SegWit) and can be thought of as the world's simplest Decentralized Autonomous Organization (DAO). It allows people to: (1) Propose upgrades, (2) Review upgrades

during a “review period,” (3) Cast votes on upgrades during a “vote period” and (4) at the end of the vote period, the proposal must pass or fail. Votes are cast by producing a block so influence over governance is based on how many tokens a user has burned, not how much they hold (stake). Application of the upgrade is delayed 1 week to ensure developers and businesses have time to adapt their systems to the upgrade.

To prevent the spamming of proposals, users must burn KOIN whenever they submit a proposal. In order to ensure this fee can be calculated in a decentralized and autonomous manner, the burn fee is equal to the total supply divided by 1,000,000. Since all actions on the blockchain must also pay a fee in Mana, the “resource credit limit” for submitting a proposal is 1/10th of the burn fee, or 10 Mana in the previous example.

Upgrading Governance

Since the governance system is itself a Koinos smart contract, all of these parameters can be changed without a hard fork. In fact, this is what ultimately distinguishes Koinos as the only blockchain truly capable of *evolution*; governance can upgrade itself! But as the most important component of the system, it should be much harder to change governance than any other part of the system. For that reason, a 75% supermajority vote is required for governance upgrades, while only a 60% majority is required for non-governance system upgrades (system call overrides and system contract promotions). But again, even these numbers can be modified by governance (with a 75% majority).

Conclusion

In this document we have outlined the innovative business logic added to the Koinos blockchain framework to make Koinos mainnet the most accessible blockchain in the world. The Mana system allows for more efficient use of network resources while creating the frictionless (even fun) user experiences to which people have become accustomed. Mana delegations allow non-token holders to use dApps without having to acquire tokens, completing the Web2 user experience on a decentralized platform. The KOIN token allows mainnet to launch fully decentralized as a result of its open and fair proof-of-work launch on Ethereum. On mainnet, the KOIN token will regulate free usage of the entire Koinos ecosystem, inflating and deflating appropriately through the proof-of-burn consensus algorithm, while decentralized governance pushes continuous improvements through fork-less upgrades developed using the Universal Language Support.