Egalcoin: A Peer-to-Peer Electronic Monetary System

egalcoin.io 𝕏 [m] Revision 2024 07 14

Michael Liesenfelt, Rob Bird, Jared Corduan, Rick Richardson, Christophe Garant

Abstract. The Egalcoin hypothesis is: cryptographic enforcement of maximum decentralization and maximum fairness are both necessary for a money destined for mass adoption and global confidence. The architecture of Egalcoin is designed to embody egalitarian economic principles algorithmically, enforcing decentralization and fairness cryptographically. We will show that all existing blockchains aren't an optimal solution for an electronic monetary system because their underpinning assumption is flawed: **currencies do not need global total ordering**. The core of the Egalcoin Monetary System is a causally consistent parallel asynchronous Byzantine Fault Tolerant Collision-free Replicated Data Type hashgraph. In contrast to a timechain of blocks, the parallel asynchronous BFT-CRDT is much more like cash enabling instant point to point transactions. Egalcoin eliminates an issuer and initial coin offering by using CPU-hard Proof-of-Work mining with stable difficulty over time to incentivize hard work and dedication rather than rewarding a lucky few who heard about Egalcoin early. CPU-hard Proof-of-Work disadvantages the use of application-specific hardware, making mining accessible on equal footing to anyone with standard computers and eliminating supply chain self-dealing. The security and decentralization incentive is based on permissionless mining of transaction fees. Egalcoin will include polling and voting for social consensus. To ensure a fair, unbiased genesis, the founders will not self-award any coins, will have no initial coin offerings of any kind, will not include any founders or multi-signature keys, and will provide substantial advance notification for the launch of Egalcoin. Additionally, Egalcoin will be developed, tested, and launched with the efforts of only volunteers, open to anyone interested in participating. Egalcoin will take no external funding and will not have a centralized administrative entity, be it non-profit or commercial. Egalcoin is intended to be *by the people, for the people*.

1 Introduction

Modern commerce has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. Historically, many nations have faced economic collapse after exploiting and abusing their currencies harming tens of millions of innocent people. What is needed is an electronic payment system based on cryptographic proof instead of institutional trust, allowing any two willing parties to transact directly with each other without the need or permission of a trusted third party. Transactions on a public ledger that are computationally impractical to reverse protect all participants. Consensus mechanisms are used in blockchain systems to achieve distributed agreement on the state of a shared ledger. The magnitude of decentralization of the consensus participants is the foundation of the block chain trilemma [Buterin] and fundamental to the integrity of a cryptographic currency.

In this paper, we propose a consensus-based electronic money in the form of cryptographic currency using a peer-to-peer distributed network to generate computational proof of the relative order, validity, and integrity of transactions without trusted third parties or institutions. Importantly, unlike other cryptocurrency systems, Egalcoin enforces maximum decentralization and algorithmic fairness cryptographically by design, rather than merely hoping for them to happen. This differentiation is central to Egalcoin's value proposition: **Ensure fairness for all and not just consensus to ensure confidence.** This electronic payment system would fulfill many market requirements including: permissionless self-banking, globally serving the unbanked, censorship resistance, a safe stable store of value, a performant medium of exchange, financial transparency, secure voting/polling, individual verification, and securing principles of the cryptocurrency industry.

1.1 Background

Historically, countless blockchains have failed cryptographic currency foundational principles and values. Bitcoin's Application Specific Integrated Circuit (ASIC)-friendly Proof-of-Work (PoW) block creation became infeasible for individuals to mine, centralized consensus to a handful of large mining pools, and lost the censorship resistance property of decentralization [BTC.com]. The Ethereum Decentralized Autonomous Organization (DAO) hack response reversed transactions and hard-forked the network in a show of centralized power and control by the affected investors [Wikipedia]. The USDC and USDT stablecoins require users to trust that the Circle and Tether companies hold adequate fiat reserves in fiat institutions and won't exercise the ability to seize the coins. Cardano began with 5 permissioned Initial Coin Offerings (ICO) in Japan [Cardano.org], included 7 genesis keys held by the 3 founding organizations to control network parameters & treasury, used a biased incentive scheme to benefit large stakeholders, and resulted in stagnant decentralization [Balance Analytics]. Solana is dominated by early investors which sacrificed decentralization and fault tolerance for quick investor profit at the expense of retail investors. The Terra stablecoin and the associated Luna reserve asset cryptocurrency functioned as a ponzi scheme which enriched the founders & investors before a collapse that wiped out almost $45 billion of market capitalization [Wikipedia]. Currently, the core problems are the centralization risks of censorship, institutional capture, founder capture, and biased unfair launches that do not reflect crypto's foundational principles and values – there is room for significant improvement.

The decentralization of block production is commonly quantified by the Nakamoto Coefficient or Minimum Attack Vector (MAV) [Srinivasan]. The practical limit of the MAV is a fraction of the total number of blocks per epoch, approximately: $MAV_{limit} \cong ½ (½ [blocks/time])$. For Bitcoin with ~144 blocks per day this would be approximately an MAV of 36/day or 252/week. PoW coins have the benefit of a permissionless launch, however mining pools for block production consensus eventually centralize to an MAV of 2 or 3. Simply put, by controlling 2 groups, the entire blockchain can be censored and permissioned. Unfortunately for Bitcoin, this centralization is unavoidable because solo-mining has become impractical for the average person. Instead, participating in mining pools, which are inherently centralized, has become the only way for the masses to participate and thrive in mining, introducing friction and corporate trust issues. Furthermore, ASIC or Graphics Processing Unit (GPU) based PoW has high hardware costs, a geographically-constrained supply chain, and unbounded energy use to mine coins more competitively. In contrast, Proof of Stake (PoS) consensus systems have the benefit of eliminating

energy waste which benefits decentralization. However, PoS coins exhibit unfair, investor-biased, permissioned ICO launches. There is currently no true fair launched commodity PoS coin. Additionally, staking reward schemes from reserve emissions or inflation benefit ICO investors and early adopters. Although PoS MAV's range from 5 to 30 compared to PoW MAV's <5, an ethical, vibrant, fair money ecosystem deserves decentralization as an intrinsic property which grows with use and adoption, instead of as one that can be manipulated to benefit a few.

During the last 15 years we have learned that shared principles, values, ethics, and integrity are necessary for people who desire the benefits of cryptographic currencies.

1.2 Principles

Individual economic freedom requires a fair and free currency. The name "Egalcoin" (or "Egal" for short) was selected for its phonetic similarity to both Egalitarianism and the Golden Eagle. Since the beginning of recorded history, humans in the temperate northern hemisphere have admired the golden eagle. The golden eagle is an apex predator cross-culturally associated with power and freedom. The word "Egalitarian" is derived from the French word "égalitaire," which in turn comes from the French word "égalité" meaning "equality." The French term "égalitaire" emerged during the French Revolution in the late 18th century when the principles of equality and social justice were being promoted. The term "Egalitarian" was later adopted in English to refer to individuals or ideologies that advocate for equality, particularly in terms of social, political, and economic rights. It represents the belief in equal treatment and opportunity for all individuals, regardless of their background or characteristics.

> *"The computer can be used as a tool to liberate and protect people, rather than to control them."* [Finney]

Adam Smith, a prominent economist, also advocated for a 'fair money' ethos, emphasizing the significance of ethics and fairness in society as a critical counterbalance to unchecked self-interest in free markets [Smith]. Similarly, Satoshi Nakamoto challenged an unfair trusted third party paradigm by replacing trust with technology for self-custody and verification [Nakamoto]. Egalitarian economic principles applied to this electronic monetary system results in a unique architectural design. Participants deserve permissionless, trustless, economic freedom and equal opportunity without systematic bias, exploitation, exclusion, or abuse. Egalcoin's principles do not include theft, systematic bias, discrimination, exclusion, censorship, or wealth redistribution.

> *"And I sincerely believe with you, that banking establishments are more dangerous than standing armies; & that the principle of spending money to be paid by posterity, under the name of funding, is but swindling futurity on a large scale."* [Jefferson]

To have a genesis free of monetary bias Egalcoin will be developed, tested, and launched by unpaid volunteers with no award of founder or developer stake. There will be no founders keys, no genesis keys, no master multisignature administrator keys, no power concentration for the benefit of the founders, and no early insider advantage. As a true commodity, there will be no permissioned centralized ICO because

100.00% of coins will be created with stable difficulty PoW. The system is secured by coin stakeholders and honest operators collectively validating transactions.

As the number of stakeholders of a cryptographic currency grows, the number of node operating participants should also grow. Ideally, the number of transaction validation nodes should exceed the number of traditional banking branch locations globally. Egalcoin could become a ubiquitous global electronic reserve currency if it becomes a trusted store of value and medium of exchange which remains secure, performant, independent, globally distributed, maximally fair, and maximally decentralized.

2.0 Consensus

2.1 Chains of Blocks

A totally ordered set of transactions grouped into blocks linearly linked into a chain with a consensus mechanism is a blockchain. Consensus mechanisms are methods to achieve a distributed agreement on a ledger or data set. Quorum-based Byzantine Fault Tolerant (BFT) consensus and Nakamoto Consensus (NC) are the two most common consensus mechanisms for blockchains. Quorum or voting based methods offer deterministic finality as long as the quorum participant set remains small. Nakamoto Consensus systems offer probabilistic finality based on Proofs of Work (PoW) resources or Proof of Stake (PoS) resources secured with Verifiable Random Functions (VRF) [Micali].

History has invalidated the original hypothesis of Satoshi Nakamoto that “Proof-of-work is essentially one-CPU-one-vote" [Nakamoto]. CPU silicon was replaced by ASIC silicon designed, fabricated, and operated with extreme centralization. The finite amount of ~144 blocks per day with the availability of fractional difficulty work proofs enabled the pooling and centralization of PoW block creation. Currently, Bitcoin has the largest market capitalization, and has highly distributed ledger across more than 50,000 nodes, however two groups (Foundry USA & ANT Group) create >51% of all blocks (MAV=2), a few companies and foundries create the best SHA PoW ASIC's, and the energy use is exceeding 100TWh/yr.

The eventual endgame for a peer-to-peer electronic monetary system is not a chain of blocks. The eventual endgame is an architecture which is fully asynchronous and parallel, doesn't have blocks, decentralizes transaction validation to tens of thousands of nodes, distributes transaction records across tens of thousands of nodes, scales transaction volume proportional to participation, and enables tens of thousands of participants to simultaneously create coins from the fixed supply and compete for fees.

2.2 Endgame BCRDT

One common assumption underpins current cryptocurrency designs: The consistency of the system must be *linearized* and globally totally ordered transactions for consensus on a single ledger. Indeed, this assumption has profound implications:

- **Linearized systems are easy** to reason about. If all participants know the ordering of all transactions and can verify them easily, double spending is impossible.

- **Linearized systems require sacrifices of speed and scale.**.
- **Linearized systems are brittle** and susceptible to various security issues that attack their dependency on consensus, such as Sybil attacks, 33%/51% majority attacks, censorship, and centralized regulatory capture.

The strongest form of linearized system is one that also requires fast *finality*, agreement by a relevant set of nodes on the value simultaneously before a change is considered final. In the naive case, simple majority quorum agreement can be sufficient, such as those found in Paxos [Lamport] or Raft [Ongaro], while in Byzantine settings, 2/3rds or *supermajority* agreement is required, such as in pBFT [Castro]. Relaxations are possible, such as those found in Flexible Paxos [Howard], which trades off majority write quorums for greater majorities in leader election quorums. The tradeoff for fast finality then is, importantly, coordination in the form of network round trips that grows polynomially with the number of participating nodes. In practice, linearized quorum systems with fast finality are limited to 50-100 nodes.

To break free of these node count limitations, Nakamoto Consensus trades fast finality for probabilistic finality to gain scale in the number of potential participating nodes. Indeed, if one ignores the needs of a currency to be used for immediate purchases, such as buying a cup of coffee, this tradeoff would be fine. In practice, the speed of blockchains is frequently raised as a fundamental limitation of the technology.

Many attempts to mitigate the speed issue in blockchains have been made by:
- Making the block sizes larger
- Making the block times faster
- Exchanging Proof of Work for Proof of Stake (e.g. Ethereum, Cardano)
- Exchanging Proof of Work for Proof of History (e.g. Solana)
- Partitioning the network and making it asynchronous (e.g. Avalanche)
- Adding hierarchies, so-called “Layer 2” networks that settle transaction batches back to the main chain

We will show that all existing blockchains aren’t an optimal solution for an electronic monetary system because their underpinning assumption is flawed: **currencies do not need global total ordering**. Guerraoui et al. proved this in 2019 [Guerraoui]. While a linearized system can conceivably be used for any application, it is *unnecessarily strong* for a cryptocurrency, riddling chain of block architectures with trade offs they never had to make to begin with.

> *“To accomplish this without a trusted party, transactions must be publicly announced, and we need a system for participants to agree on a ~~single~~ history of the order in which they were received. The payee needs proof that at the time of each transaction, the majority of nodes agreed it was ~~the first~~ received.”* [Nakamoto]
>
> Note: Excluding only 3 words transforms a single linearized global total ordering ‘timechain’ system to scalable parallel causally consistency as long as double-spending and supply attacks are detected and prohibited.

Currencies are Causally Consistent

Readers may find their own personal experiences with currency more intuitive. If you are spending and receiving currency, what matters is your personal ledger, the ledgers of those you are receiving currency from, and the ledgers of those you are sending currency to. This form of locally-relevant consistency is called *causal consistency* and is slightly weaker than linearized consistency because there is no global total ordering across all ledgers. For example, a causally consistent system cannot be used as a lock service because independent events can happen in parallel. Only some aspects of the monetary system, like an enforceable governance, require consensus.

Endgame is the first permissionless causal consistency

By choosing the optimal consistency level for a currency, Endgame causal consistency enables remarkable properties that are simply impossible for any linearized chain of blocks to achieve, namely:

- Instant cash-like person to person transactions
- Linear scaling of transaction rates by node count
- Wire-speed single transaction latency
- Immunity to Sybil attacks
- Immunity to 51% attacks
- Full node security for light clients

Put simply, Endgame causal consistency is the appropriate solution for a peer-to-peer electronic currency. A linear chain of blocks is replaced with a Byzantine Fault Tolerant Conflict-Free Replicated Data Type (BFT-CRDT or BCRDT) providing global parallel asynchronous causal consistency for Egalcoin.

Byzantine Fault Tolerant Conflict-free Replicated Data Types

A Conflict-free Replicated Data Type is a data structure replicated across multiple networked computers with the following properties:

– Any replica can be updated independently, concurrently and without coordinating with other replicas.
– An algorithm operating on the data automatically resolves any inconsistencies that might occur.
– Although replicas may have different states at any particular point in time, they are guaranteed to eventually converge.

> "*Making CRDTs Byzantine fault tolerant does not require a redesign of the algorithms: it is possible to retrofit BFT to existing CRDT algorithms with some modest tweaks, without changing the fundamental way how they work*" [Kleppmann pdf].

Every update must contain a set of preceding dependency ID's including the ID of the previous transaction. This graph of updates must be built with unique ID's that are not susceptible to Byzantine misbehavior. Each transaction ID is generated using a strong cryptographic hash of the entire contents of the transaction. Each transaction will include the total transaction count of the address. Simply put, the transaction count is very similar to the unique incremental check numbers on each check of a personal checkbook. The hash graph of transaction dependencies is assembled on a per-address basis, not attempting to replicate a global total ordered and sequenced timestamp chain. A collection of address

counts becomes an integrated version vector [Parker] which collectively functions as a distributed vector clock [Lamport]. Every address becomes its own transaction chain.

Strong Eventual Consistency
Both Nakamoto Consensus and the BCRDT model are based on Strong Eventual Consistency which requires: Eventual delivery, Convergence, and Termination. Nakamoto Consensus offers probabilistic finality which eventually reaches strong consistency after a duration of 6 to 10 successive block intervals. The BCRDT offers strong eventual consistency at the speed of gossip intervals across the network, which is much faster than block-based Nakamoto consensus. As long as all honest participants are connected with one or more network paths, all honest participants will eventually converge to the correct state. Even new participants with only the founding BCRDT transactions at Genesis will converge to the correct state.

Participants are free to directly transact by exchanging histories and portions of the hash graph. Relative to an honest sender, transactions are final immediately upon signing, adding to the local chain, and broadcasting. Relative to a receiver the transaction may be directly received from the sender and broadcasted or random network peers could deliver the transaction from the P2P network to confirm successful distribution. Global consensus mechanisms, limited memory pool sizes, fee markets, and censorship cannot prevent honest Egal participants from conducting a transaction, exchanging histories, and gossiping the update globally. Honest participants can transact offline or via Near Field Communication (NFC) and delay broadcasting new transactions making Egal a cash-like barer asset. If a Byzantine participant behaves in a way which leaves cryptographic evidence of malicious behavior, such as a double-spend attempt, all faulty transactions will be recorded and permanently tombstoned or slashed at the speed of network gossip. Simply put, if you sign two checks with the exact same check number every honest node will remember the violation and ignore checks from your checkbook forever.

3 Monetary Policy

There will be no issuer, no Initial Coin Offering (ICO), no founder's allocation, no foundation allocation, no automatic coin distribution, and no taxes to ensure that this coin is not designed to make the founders, investors, and/or a political class wealthy. Egalcoin will use constant-difficulty-over-time PoW to enable participants to create their own coins up to a fixed supply limit.

3.1 No Issuer, No Initial Coin Offering

Egalcoin will not have a centralized issuer or Initial Coin Offering (ICO). Because a sybil-proof global identity system does not exist, the permissionless method of acquiring tokens must be a computational PoW entirely at the protocol layer. Before Bitcoin, PoW technology was originally proposed as a solution for email spam [Back]. Bitcoin used PoW technology for both consensus and distribution simultaneously. Work proofs bundled into individual transactions enable the permissionless individual creation of commodity money without a centralized permissioned ICO. Work proof transactions will be required for creating all coins and every participant must prove work as a true commodity. To prevent unlimited energy use and prevent monetary supply exploitation, the total coin supply and total number of potential

work proofs would be finite. Coin creation using PoW transactions enables distribution to many participants simultaneously at a steady difficulty which eliminates ‘satoshi coins’ advantages.

> *“The ~~steady~~ addition of ~~a constant of amount of~~ new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended.”* [Nakamoto]
>
> Note: Portions of the quote were excluded because the mining rate of gold changes based on market conditions and extraction price point. Bitcoin chose a “steady” “constant amount of” new coins bound to consensus, however Egal mining will be more like gold mining with a variable market-driven market rate with stable mining difficulty for fairness.

Coin distribution using PoW instead of an ICO solves two problems simultaneously: a reasonably fair permissionless decentralized creation of coins and minimizing early insider advantages. To limit centralization, a CPU and memory-heavy PoW method will discourage the use of specialized hardware like ASIC’s, FPGA’s, and GPU’s. The PoW difficulty should be as consistent as possible so early adopters won't have a large advantage against those who mine later.

The cost of replacing a centralized ICO with decentralized permissionless PoW is the storage of all work proofs. Utilizing 2,000GB of uncompressed ledger space for <100 Byte work proofs would result in 20B work proofs for creating coins with PoW.

3.2 Coin Creation: RandomX PoW

> *“We should have a gentleman's agreement to postpone the GPU arms race as long as we can for the good of the network. [...] It's nice how anyone with just a CPU can compete fairly equally right now.”* [Nakamoto]

No computational proof of work algorithm will be perfect for permissionless decentralized mining of coins. Egalcoin will use the RandomX PoW algorithm developed for Monero [Tevador]. RandomX is optimized for general purpose CPU’s with memory-heavy techniques which utilize random code execution and ample amounts of L1, L2, L3, and DRAM per thread. RandomX was specifically designed to discourage the use of specialized hardware with the intent of enabling a more egalitarian distribution of coins. RandomX is capable of $O(10^3 - 10^5)$ hashes per second on modern processors which would enable the validation of every PoW transaction in every block. Efficient mining would require:

- A 64-bit architecture
- IEEE 754 compliant floating point unit
- Hardware AES support (AES-NI for x86, ARM Cryptography extensions)
- 16KB of L1, 256KB of L2, and 2MB of L3 per thread
- Support for large memory pages
- At least 2.5 GiB of free DRAM per NUMA node

In order to create coins miners will create proof solutions for each of the 20e9 available mining opportunities. For ASIC resistance the RandomX K parameter will be based on the cumulative cryptographic hashes of previous sets of transactions. Each new coin creation must be linked to prior PoW coin creation transactions added to the BCRDT graph and traceable back to genesis according to:

RandomX(K , H) < **`PoW_Difficulty`**
N = work_unit_number[1 .. 20e9]
K = hash(PoW(2^(floor($\log_2$ N)-1 as usize))) || .. || PoW(2^(floor($\log_2$ N as usize))))
H = hash(miner_address || PoW_claim(N>>1) || K || N || nonce_value)

3.3 Native Currency

The blockchain's Native currency [Eg , ∈] will adhere to egalitarian hard money principles. The smallest single integer unit of ∈1 would be called an eaglet. The divisibility for Egalcoin is one part in $10^{15.0}$ compared to Bitcoin at one part in $10^{15.3}$, the US dollar at one cent in ~$10^{15.3}$ cents [M2SL], or Gold at 1 gram in $10^{11.3}$ grams. Technologies for Gold micro-layer vacuum deposition onto polymer sheets can increase the divisibility of physical gold to the scale of 1 milligram in $10^{14.3}$ milligrams [Valaurum]. There will be a total supply of 1,000,000,000,000,000 (1,000T) indivisible integer ∈ units, on average ∈100,000/human for 10B humans. If the **`PoW_difficulty`** was tuned such that each work proof requires on average 5kWh of energy to generate using RandomX, then approximately 100TWh would be required to mine available supply. Each work proof would create ∈50,000 and cost approximately 5kWh, so the approximate ratio at genesis would be ∈10,000/1,000Wh.

To be fair money, ∈ will need to adhere to the four functions of money: a medium, a measure, a standard, and a store [Jevons]. The medium of exchange is provided by the peer-to-peer decentralized networking. The common measure of value is established by the fixed supply and smallest indivisible monetary unit, ∈1. Egalcoin will provide the stable store-of-value property using memory-hard stable-kWh-difficulty work proofs and free market price discovery at a rough order of magnitude of ∈10,000/1.00kWh until the entire supply is mined. Stable kWh difficulty means that early miners will not have massive compounded advantages and ~5kWh of energy will create ∈50,000 for a long period of time. Free market forces between the mining price and the market price would likely keep this ratio stable until the entire supply was mined. Mining difficulty will slightly and steadily decrease in difficulty over time with the availability of faster CPU and memory, however without a revolutionary advancement of material science beyond silicon (eg. diamond, superconductors) these improvements will be predictable and incremental.

Bitcoin meets three of four criteria (a medium, a measure, and a store), but historically has not provided a stable standard of value. BTC has experienced large price changes due to speculation, manipulation, variable mining difficulty, and centralization of privately created superior ASIC generations. Numerous algorithmic and fiat backed stablecoins have emerged in an attempt to provide the stable standard of value property. Miners must eventually sell coins to pay the bills for a PoW consensus chain, however low resource requirement consistency gives miners the incentive to selectively and sustainably choose when and how to mine. Egalcoin provides a stable standard of value via stable difficulty PoW mining until the maximum supply is reached. After the maximum supply is reached a stable standard of value is established by a high degree of stakeholder decentralization and free market value determination.

It could also be argued that a digital currency exhibits a fifth core value function: security. Self-custody is the most important feature for knowing that your money is secure. Egalcoin will have trustless security in self-hosted P2P full-node wallet(s) that can be used for self-auditability, self-custody, self-mining (no pools), and self-participation. Egalcoin will provide peace-of-mind security by empowering individual users to participate and propagate the network.

3.4 Incentives

> *"Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free."* [Nakamoto]

The first and most important incentive is to individually mine and create the coin commodity. Each work unit would create ∈50,000 in contrast to the first Bitcoin blocks creating 5,000,000,000 sats (₿50.0). Delegated PoS infrastructure including stake pools, stake keys, and wallet delegation to collect automatic reserve disbursements is unnecessary when participants can reasonably mine their own coins with ~5kWh of electricity. The initial coin creation mining process will bootstrap the P2P gossip network and BCRDT replication. After all coins are mined a market-based fee economy will be necessary to incentivise maximum gossip and history replication participation.

> *"If you're sad about paying the fee, you could always turn the tables and run a node yourself and maybe someday rake in a [ ] fee yourself."* [Nakamoto]

There is no perfect method for handling network fees, even though some nonzero fee is necessary to financially discourage dusting attacks or wash trading. The rationale is for fees to be approximately 1-2 orders of magnitude cheaper than traditional centralized finance & banking services, but not so cheap that the fee-based incentive for decentralized security is eroded. A fee should scale proportionally to only the `amount` of native currency sent to a new address, but not the amount returned to the input address. Fees per transaction would be:

```
Tx_Fee = MAX( floor(fee_per_byte*tx_bytes) + fee_per_tx , floor(0.1%*amount) )
```

Time durations cannot be used as a fee claiming criteria because the BCRDT does not have a forced global time clock or forced measure of time. The fee of each transaction will be claimable by the best PoW solution when each transaction becomes buried 2 layers deep within the hashgraph. The best PoW solution will be based on the cumulative transactions of each address to promote history retention.

MIN(RandomX(K , H))
K = H(Tx_0 || ... || Tx_N)
H = miner_address || nonce_value

This approach aligns the entire Egal mining community with the long term operation, decentralization, and storage of the network with a fair, permissionless, competitive, and market-based incentive mechanism. Operators could choose to mine all or select transactions of any size or value. The long-term

duration of the fee mechanism encourages long-term history retention and enables intermittent or seasonal renewable energy use for PoW. A fixed fee amount will effectively limit the total fraction of the financial system spent on energy to maintain the financial system.

4 Network

4.1 Random Graph P2P

> *"Governments are good at cutting off the heads of a centrally controlled networks [ ], but pure P2P networks [ ] seem to be holding their own."* [Nakamoto]

Fully decentralized and distributed Peer to Peer networking is necessary for the success of a cryptographic currency. A P2P random graph topology is necessary to avoid supernodes, information asymmetries, transaction front-running, and censorship while scaling the network to millions of nodes. The P2P network cannot centralize to large, fast, institutional peers. Ideally, P2P nodes will become more numerous than all bank and currency exchange branches globally. Egalcoin will use a P2P random graph topology from genesis with no central points of failure and no dependence on centralized DNS services. To aid network discovery for new peers, IPv4/IPv6 addresses and ports can be included in the on-chain metadata of transactions.

Peer lists, new transactions, and contents will be shared between peers using diffusion gossip. Bootstrapping new peers from genesis would be safe using just the genesis BCRDT. The network must preserve maximum fairness while maintaining optimal resilience, speed, and scaling properties. The P2P network should converge to a maximal expander random graph which is fair between all potential participants of any stake amount. Participants are full or partial nodes with bi-directional random graph P2P communication to any number of other random or explicit participants. For Distributed Denial of Service (DDoS) attack mitigation all participants will have connection limits, per connection rate limits, and temporary blocklists.

Peers will self validate the accuracy and quality of their P2P connections by comparing the accuracy, proof of work claims, time to arrival / conductivity, and transactions from many different subgraph partitions. Eventually, peers will not be able to contain the entire global BCRDT, so nodes will 'subscribe' to subsets of address prefixes. All transactions would contain a random 64-bit nonce field to ensure each participant could always generate a transaction ID with their preferred prefix. Address prefixes could be related to GPS or location coordinates.

5 Structure

5.1 The Genesis

The transactions at the Egalcoin genesis begin the BCRDT will be unique and manually created. The total circulating supply will begin at ∈0. At genesis each volunteer will begin PoW mining their own coins

using the blockchain global **`parameters`**. Each participant will include unique metadata and timestamp information. The current newspaper headlines or hash values of other blockchains could be included in the metadata. There will be substantial advance notification of the genesis convention to the broad community before replicating the genesis BCRDT globally to begin Egalcoin monetary system. Cryptographic hashes of the genesis PoW transactions would become an initial source of shared entropy for the monetary system.

The genesis would establish the initial global **`parameters`** set:

- `protocol_version : 2026.0 ( 0.0 , 1.0e9 )`
- `total_coin_supply : 1e15 ( 1e15 , 1e15 )`
- `max_transaction_size : 16384 [B] ( 4096 , 131072 )`
- `PoW_difficulty : ????? ( ? , ? )`
- `fee_per_byte : 1.0 ( 0.01 , 100.00 )`
- `fee_per_amount : 0.001 ( 0.0001 , 0.0100 )`
- `fee_per_tx : 1 ( 0 , 1000)`

The **`protocol_version`** parameter enables governance for protocol updates. Operators would be able to upgrade node software and indicate their supported **`protocol_version`** in transaction headers.

5.2 Unspent Transaction Outputs and Accounts

Bitcoin introduced the Unspent Transaction Output (UTxO) model, such that each transaction contains one or more inputs and one or more outputs, allowing value to be split and combined. Extended UTxO or eUTxO was developed to extend and mix native currency transaction inputs & outputs and all other digital asset & token type inputs & outputs natively without smart contracts [Chakravarty]. For example, dozens of NFT's, FT's, digital asset tokens, and native currency outputs can be combined into a single transaction [eUTxO.org]. Blockchains using eUTxO have executed 10,000 outputs in a single transaction [Ergoplatform]. The UTxO model is most similar to a cash or coin ledger system.

Every person with a physical wallet will carry a collection of cash, coins, account cards, identity cards, membership cards, and even personal mementos. Egalcoin will be a 'Chimeric' which will combine both an account and eUTxO model to reflect this reality [Zahnentferner]. The account model would be a single reused address. The eUTxO model will offer significant advantages for some use cases while the account model will offer significant advantages to L2's, programmability, and institutions. The BCRDT hash graph structure most closely represents an eUTxO hash graph structure.

5.3 Digital Assets & Exchange

Native Digital Assets and Tokens (DATs) are necessary to represent classes of traditional instruments including: commodities (like gold), securities (like stock certificates), identities (like memberships), and property (like deeds and art). DATs enable the replacement of trust-based traditional institutions, courthouses, banks, and brokerages with on-chain programmable and functional ownership. DATs should be governed by the **`policy`** and **`asset`** keywords which control the minting and burning policies.

DATs should not be created for free. Creating indefinite quantities of DATs for nothing leads to intra-chain asset inflation and extraction of native currency value. The creation of each unit of a DAT policy shall cost ∈1. The destruction or reclamation of each DAT unit shall yield only ∈1.

5.4 UI/UX

A full node wallet reference implementation should have an intuitive user interface requiring no power shell or terminal skills. All of the necessary tools and metrics will be included to empower every user. The interface will look and feel like the Monero reference client, but with a few extra menus and options. Mining new coins via PoW would be enabled with a check box, and selecting the address to mine to. Full nodes can choose to add a participation transaction to the BCRDT.

> *"You can get coins by getting someone to send you some, or turn on Options->Generate Coins to run a node and generate blocks."* [Nakamoto]

The wallet GUI shall provide dialog screens for trustless verification of: key metrics, mining & circulating supply, transaction search, network & protocol status, and voting. Users will be able to perform simple and scripted queries to generate statistics, create custom alerts, and even create dashboards.

5.5 Voting

Every participant will have the right to decide the future roadmap of Egalcoin. The founders and developers will not retain any powers or control of the architecture after genesis. A robust polling mechanism would allow every stakeholder to create any poll as a platform for social consensus.

Any stakeholder would be able to submit a `poll` transaction with multiple selections. These polls would have no protocol level automatic interpretation and enactment instead serving as a feature for social consensus. Individuals would be able to cast a `vote`. The submitter of the `poll` will specify how votes will be counted (ex: stake, voter count/identity unweighted or weighted geometrically/quadratically), the beginning of the voting period, and the end of the voting period. The submitter would also be able to commit a concluding summary of the poll. Voting and polling becomes a key feature for enabling decentralized development priorities and the freedom of expression through voting.

5.6 Programmability

The programmability of the platform must provide an efficient, secure and easy way to implement financial contracts. There is a tradeoff between the complexity of a programmable environment, the potential attack surface, and the resulting security of the environment. Also, for developer onboarding there is a tradeoff between environment familiarity and developer adoption. The standard library of the programmable environment must contain all necessary cryptographic primitives, hash functions, signing functions, math functions, ZKP functions, and utility functionality. ErgoScript is an example of a scripting language which is used to specify the conditions under which currency can be spent [ErgoScript]. ErgoScript supports a type of non-interactive zero-knowledge proofs called Σ-protocols which supports

ring-signatures, multi-signatures, multiple currencies, and atomic swaps. A well behaved non-turing-complete scripting language will cover >90% of use cases and functionality while being less complex, more secure, and computationally efficient.

5.7 Privacy and Identity

The spectrum of privacy and identity technologies is very important and contentious. Authoritarians desire centralized search and seizure powers over money, transaction & voting information, and permissioned control of identity. Freedom respects secret ballot democratic voting, the privacy of cash & electronic equivalents, the personal ownership of identity, and protections from unreasonable searches & seizures. Zero Knowledge Proofs (ZKP's) are a freedom-enabling technology for secret ballot voting, decentralized identities, and private cryptographic currency transactions. There are legal and valid institutional and individual motivations for both centralized and decentralized privacy and identity capabilities.

> *A Cypherpunk's Manifesto "Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world."* [Hughes]

Egalcoin's open source & permissionless architecture and programmable capabilities won't be able to prevent global participants from implementing existing ZKP privacy, confidential identity, or secret ballot voting capabilities. Somebody somewhere in the world will eventually implement existing privacy and identity technologies, however the US-based authors of this whitepaper won't create new privacy or identity solutions risking years of unethical incarceration, guilty treatment, and theft until a delayed court date just to reassert open source software freedom of expression first amendment rights [EFF].

5.8 A Treasury

A treasury is a mechanism for a majority to tax the transactions of the entire global network for treasury spending deemed necessary by the majority. A couple of important principles must be respected including: 'No taxation without representation' and 'don't be evil versus cannot be evil'. Taxation, a treasury, and voting on budgets can become highly political and susceptible to centralization, bias, enrichment, and corruption. There will be no source code, blockchain parameters, or balances to support a treasury at genesis. If there is on-chain democratic consensus for taxation a future hard fork or network segmentation will be required to include a tax and a treasury. Egalcoin will be built by volunteers and updates to Egalcoin can be contributed as volunteer efforts without the need for taxation or treasury compensation.

5.9 Post-Quantum Cryptography

Digital signature schemes are built on one of three hard mathematical problems: the integer factorization problem, the discrete logarithm problem, or the elliptic-curve discrete logarithm problem. All of these problems could be solved on a sufficiently powerful quantum computer. If or when a sufficiently powerful

quantum computer is created, every unit of value on the ledger would need to be transferred and signed with a new post-quantum cryptography (PQC) signature scheme.

Starting in December 2016 the US National Institutes of Standards and Technology (NIST) issued a public call for quantum-resistant public-key cryptographic algorithms [NIST]. After three rounds of evaluation NIST selected three digital signature schemes. In September 2022 NIST issued a fourth call for additional digital signatures. After the June 1st 2023 deadline 40 submissions met the requirements. NIST anticipates the fourth round of evaluation lasting several years with a fifth PQC standardization conference in April 2024. The quantum resistant digital signature scheme will likely be based on the round-3 finalists of: FIPS 204 Module-Lattice-Based Digital Signature Standard or Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU lattices.

Blockchains do not have the available block space to accommodate a complete signature transition of every participant to much larger quantum resistant signatures in a reasonable amount of time. Egalcoin with the Endgame BCRDT would enable every participant to upgrade to quantum resistant signatures on the same day. The P2P network would be stressed gossiping the newer larger signatures for every address at maximum capability, but the security and integrity of all participants would be protected. Therefore, Egalcoin will support both an elliptic curve and a post-quantum signature scheme, however smaller elliptic curve signatures will remain the default until a viable quantum computer is demonstrated.

6 Conclusion

Individual economic freedom requires a fair and free currency. Egalcoin builds upon and corrects the giants before us. The Egalcoin hypothesis is: Real world use and mass adoption of money requires a belief in the fairness of money and complete decentralization. The 'product-market fit' for money to achieve 'mass adoption' is complete decentralization. Ideally, the number of nodes participating should exceed the number of traditional banking branch locations globally.

The native token currency [Eg , ∈] will adhere to egalitarian hard money principles. A finite Earth cannot sustain a population or a money supply which grows forever. To be fair money, ∈ will need to adhere to the four functions of money: a medium, a measure, a standard, and a store with the added property of security. To be fair, ∈ will be created by volunteers with no founders' stake. To be fair, the founders will not retain any power or control with genesis keys. To be fair, ∈ will use permissionless work proof claims to eliminate a permissioned ICO. To be fair, ∈ will prevent network censorship or information asymmetry advantages. Permissionless uncensorable voting and polling is necessary for the freedom of individual expression and decentralized freedom of expression.

Somebody has to improve the ethical standards and principles of the cryptocurrency industry because the benefits for humanity would be world changing.

🦅🪙, Fair money.