Table of Contents

Cotidianus Digitalis (CODI): the modern solution to money

Introduction

In this paper, we will give you reasons to invest time and money in one of the most promising enterprises of the future: A digital currency that works worldwide for everyday people in their everyday lives!

We will outline a new digital currency that will use the enormous technological advantage of the last decades to get rid of the known shortcomings of money-systems used by mankind so far, while keeping the advantages they had for their users.

Unlike other digital currencies which we have seen in the past 20 years, CODI is meant not as a playground for speculation but as real money meant for real people.

We are completely aware of the fact that such promises must sound like madness, hubris, or, even worse, marketing!

But we are confident that CODI can counter all technical, practical, and economic criticisms with little difficulty!

A note on the presentation:

In creating this white paper, we have consciously chosen to focus on the clarity of thought and the precision of language. We want to spare you the "glossy" diagrams and "shiny" photography often found in modern presentations, as we believe they can sometimes become tiring and distract from the core logic.

Remember: History's greatest thinkers and writers managed to articulate their most complex arguments and profound principles through the power of the written word alone.

Following this tradition, we will only set aside the English language if we can replace it with the even greater precision of mathematics.

If your time is precious, you may skip the historical outlook and move directly to chapter 2!

For all others, you may enjoy a stroll through history with us, as this is not only interesting in itself but might also help you to understand the reasons why we constructed CODI the way we did and build insights into its properties from the bottom up!

1. Mankind's money systems and their Pros and Cons

1.1. Coinage from precious metals

For the ancient Greeks, Romans and their neighboring cultures, pure silver was the way to go: a silver coin consisted usually of 95% silver and 5% copper.

This simple and elegant system provided huge advantages:

it was a safe, universal, reliable & stable value useable across all times and nations!

Safe:

Pure Silver has a shine that is impossible to copy by other metals, even with today's methods. So just by the looks a merchant in Alexandria or Athens could see that it is real silver!

If he wanted to be extra sure, he could e.g. bite on it to test its softness - the reason many ancient coins have bite-marks. This way, silver-plating (a technique known already in these times, usually done with the help of mercury) could be ruled out since copper or other metals were harder.

Universal:

Wherever and whenever silver was discovered in a culture, it was considered valuable!

So wherever you were in ancient times, you knew your silver would provide a real value there!

Reliable:

Silver-coinage provided a safety from government-actions that is almost unthinkable today! Whatever happened in the world of war and politics, the value of your silver coins was completely unaffected by it - for the very simple reasons that your coins could be melted and formed into something new - spoons, jewelry, plates and cups, whatever you wished and it took no more than a half-competent blacksmith. And, should times change again, your silver-ware could be re-melted into coinage again!

So, your city might have been burned to the ground and its coinage banned for all times by all the gods, yet at least your silver kept its value!

Stable:

Inflation was practically impossible with silver-coinage, as it was difficult to mine and its amount thus relatively stable over times.

Yet, for all its advantages, there are good reasons why we don't use silver coins anymore:

It is completely impractical for daily use and unable to grow with the modern economy.

Impractical:

Imagine buying a cucumber, a small coffee or an ice cream for your kids with silver coinage - impossible, for even the smallest silver coin we know would be way too valuable for this! You would have to pay with silver grains! For this reason, all economies using silver coinage had to introduce a second set of coins made from much less valuable metals like copper or brass. But with these, none of the advantages above applied: they were rather easy to counterfeit and their value was more doubtful - good enough for everyday use and shopping, but not for more.

Needless to say, having two different currencies, one good and one rather bad provided numerous problems! And these grew only worse because of the second disadvantage:

Unable to grow:

The amount of silver is rather fixed.

That is great for keeping its value, but leads to constant deflation, because the population and the amount of valuable goods produced increases always! Mankind is industrious!

Thus, the single silver coin in your purse grows ever more valuable and with it, more impractical for everyday life!

1.2. Fiat money

As the economy, population and technology evolved, mankind needed something else and this came in the form of Fiat money. The history of it being a complex one, but some factors always stayed the same:

A central agency, backed by the highest authority of the state, issued currency that derived its value from the fact that it was legal tender in this country. Thus, it provided:

A practical, completely scalable currency in which the amount of money could always be adapted to the need of the economy!

Practical:

No more need for heavy metal with this money, it can be printed on featherlight paper-bills that carry all day in every purse or transferred digitally online.

Completely scalable:

Be it pennies or billions, this currency always has you covered. Easy to produce pennies and dimes for the candy for the kids, a signature or a push of a button to move millions and billions in the blink of a second!

The amount of money could always be adapted to the needs of the economy:

This is the key strength of the Fiat system and the main reason it is used in all economies of today! Whether you go to a war, experience an economic downturn or an unprecedented decade of boom, the Fiat system can always deliver!

But, here, too, there are a lot of thorns that come with the roses:

It relies on centralized power of the state, is thus prone to political influence and heavily tends to inflation!

Relies on centralized power of the state:

Usually, this happens via a form of central bank. Though the exact setting of this bank varies from state to state, the problem is always the same - a very, very small number of people with at best indirect democratic legitimacy decide on the money of dozens, if not hundreds of millions of people! To the free-thinking, this is almost unbearable! Even if central bankers were directly voted into office, this would only decrease the lack of democratic legitimacy, but not the problem of huge power concentrated in the hands of very few.

Prone to political influence:

Routinely, governments do everything in their power to ensure that the “independent” central banks work the way they want them to do! This is a yearly “soap opera” with

much entertainment to the political establishment, but little good to the economy because it very often leads to the last and most harmful consequence of Fiat money!

Heavily tends to inflation:

Fiat money has an almost inevitable tendency to create inflation. Looking up the data of modern economies of the last 50 years, you will be very hard pressed to find more than three examples of deflationary national currencies! Switzerland and Japan are the only countries not suffering from much inflation, and they serve as the exception that confirms the rule!

Because central banks in the end serve governments, and governments always, always, always need more money, there is always money to be printed and interest rates to be lowered!

While this is just a nuisance when times are good, it becomes a true horror in times of crises, whatever their nature! Germany in the 20s, Venezuela just recently, numerous African states and of course the West during the Corona-pandemic: History is full of stories of out-of-control inflation which have hurt countless people whose savings lost all value right before their eyes and often destabilized entire societies!

1.3. Frankenstein's monster or The Gold Standard

To end our short monetary history, we can't avoid talk about the most absurd proposal to end the worries of modern money: the Gold Standard and its derivatives!

We must admit that this is a rather unpleasant excursion, since the Gold Standard was praised by people who doubtlessly contributed much to the modern world: David Ricardo, von Mises, von Hayek and so on.

While we do not in the least doubt the great insights of these brilliant minds in other fields of society and economy, we seriously dismiss their praise for the Gold Standard!

We only see one good in the use of the Gold Standard, and this was its universality, thus making exchange rates between countries very predictable and immune to the speculation we often see today.

Otherwise, the Gold Standard was the Frankenstein's monster of money theory: stitched together from pieces in the vain hope that the result would somehow be viable!

Alas, it wasn't!

It combined cleverly and effortlessly the disadvantages of all other money systems: it was as inflexible as silver coinage, but as useless in times of crises as Fiat money - no Gold Standard has survived a great war or a great crises, as it was much easier to simply dissolve the peg it relied on! And what seemed like a guarantee to gold ended up being just paper!

1.4. Lessons learned!

While history is an interesting subject in its own right, its main use is understanding the present and helping to pave the way for a better future!

We see the way of improving in financial and monetary matters by understanding the virtues of the known money systems, how they were achieved and seek a way of combining them all!

Thus, we came up with the following list of requirements a modern money must fulfill:

1. It must have an intrinsic value like silver by being useful to many people across time and borders.
2. It must be useable for something different than being money just like silver was useable for dishes as it was for coins, thus contributing to its intrinsic value.
3. Just like silver coins can be melted into spoons and then be melted back into coins, it must keep its intrinsic value no matter its current state of use.
4. Like silver, it must be decentralized, independent of government-policy!
5. Like silver, there is no easy way to mint it, keeping its value stable.
6. Every silver coin was easy to verify in its value and so must modern money be
7. Like Fiat money, it must be scalable in every direction, allowing the purchase of candy as well as ocean fleets.
8. It must be as practical as Fiat money : pennies, cheques, and online-transactions have to be in the repertoire!
9. The amount of money must be flexible, adaptive to whatever modern markets require!
10. And, last but not least: it must be absolutely peg-free to avoid the horrors of the gold-standard. By being well-useable in every country on earth, it will mitigate exchange-rate problems even better than the gold standard ever did!

In summary, the ideal form of money should embody versatility, intrinsic value, decentralization, ease of verification, scalability, practicality, flexibility, and global usability without being tied to any specific standard or peg!

We flatter ourselves with the achievement of creating a currency that does exactly that. Let us show you how it is done!

2. Why Cotidianus Digitalis is the next evolutionary step for money

2.1. CODI and Cryptography

The decisive feature of CODI is its digital intrinsic value:

We base the value of our currency on providing numbers for cryptography!

Cryptography will always be used in our modern world, thousandfold for everyday digital encounters. And it will always be in need of large numbers or, to use the technical term, "entropy." And it's not just any numbers, which will be our "silver"!

But how can this be achieved? How can a number always be valuable, no matter circumstances or usage?

To explain this, we must explore modern cryptography!

2.2. Modern cryptography

Modern cryptography is quite different from what we normally associate with cryptography: secret agents, concerned diplomats or wounded soldiers punching an urgent message into the "Enigma" or another machine!

Instead, it is used absolutely everywhere: you are not aware of it, but almost any relevant action done online uses cryptography in one way or another - a website or a download confirming its identity, a messaging service sending your "Smiley" Emoji to your aunt or uploading the picture of your dish and of course all transactions involving money! This mostly happens without you even having to use a password, which is why cryptography, despite its omnipresence in the digital world, barely crosses our mind.

2.3. Current Standards in Entropy Sourcing

In modern cryptography, the security of any system is only as strong as its Initial Entropy Source. Currently, developers rely on the following four primary methods:

2.3.1. OS-Level CSPRNGs (The Most Common Way)

Most developers use built-in Cryptographically Secure Pseudorandom Number Generators (CSPRNGs) provided by the operating system (e.g., /dev/urandom on Linux/macOS or BCryptGenRandom on Windows).

- Mechanism: The OS collects "noise" from hardware events (keyboard timings, disk interrupts) and processes it through a hash function.
- Pro: Fast, free, and integrated into every programming language.
- Contra: The "Black Box" Problem. It is impossible for a third party to verify whether the OS noise was manipulated or if a hardware backdoor (at the CPU level) is biasing the output.

2.3.2. Hardware Security Modules (HSM) & TRNGs

High-end security environments use dedicated hardware (True Random Number Generators) that samples physical phenomena like thermal noise or radioactive decay.

- Mechanism: Pure physical randomness is converted into digital bits.
- Pro: Extremely high entropy quality; physically unpredictable.
- Contra: Expensive and Centralized. Requires specialized hardware that cannot be easily audited by end-users. The user must trust the manufacturer (e.g., Intel, Thales) that no "kill-switch" or "master-key" exists.

2.3.3. NIST-Standardized Deterministic Generators

Many regulated industries use NIST-approved algorithms like Hash_DRBG or HMAC_DRBG.

- Mechanism: Algorithms that expand a small "seed" into a large sequence of numbers using standardized math.
- Pro: Fully compliant with government regulations (FIPS).
- Contra: Political Vulnerability. History has shown (e.g., Dual_EC_DRBG) that these standards can be intentionally designed with mathematical "backdoors" accessible only to specific intelligence agencies.

2.3.4. Public Entropy Beacons

Some decentralized apps use public "beacons" that broadcast random numbers at set intervals.

- Mechanism: A network of servers produces a joint random value.
- Pro: Transparent and publicly verifiable.
- Contra: Latency and Privacy. Users have to wait for the next "pulse," and since the number is public, it cannot be used directly as a private key - only as a seed that everyone knows.

2.4. CODI's USP

This leads to the question: how can CODI improve upon these systems? What is there we can offer that is so universally valuable as silver was in ancient times?

*CODI provides high-grade security that is **fully transparent and independently verifiable by any user, at any time.** Unlike traditional systems that require trust in manufacturers or central authorities, CODI's architecture allows every participant to mathematically audit the integrity of the entropy provided. It is not just independent; it is **inherently verifiable!***

This is achieved by providing cryptographic entropy for the three most used cryptographic functions!

These functions are:

1. Lattice-based Cryptography
   (e.g., Learning with Errors – LWE, Shortest Vector Problem – SVP)
   The foundation for post-quantum-secure encryption and signatures (such as Kyber

and Dilithium) as well as advanced zero-knowledge proofs and fully homomorphic encryption.

2. Hash-based Cryptography
   (e.g., collision-resistant hashes, Merkle trees)
   Essential for integrity checks, digital signatures, and proof systems – already quantum-resistant and permanently relevant.

3. Elliptic Curve Cryptography (ECC)
   (e.g., secure curve parameters, safe primes for key generation)
   The current standard for public-key systems and signatures (ECDSA, ECDH) and a key component of hybrid post-quantum solutions.

All three of these are considered computationally infeasible, two even if such things as quantum computers were ever to exist!

The strength of our offer is that we use a number that has value for all three functions!

That way, no matter which function our cryptographer uses, or even if he uses two or all three of them, he can be sure that our coin with its encrypted number in it will be of use for him and he doesn't have to waste precious time and processing capacity to find it himself.

A CODI coin is not a finished cryptographic product, but rather certified, high-performance entropy—the "high-purity silver" of the digital age. Its value lies in its verified quality and immediate usability as a universal seed. Just as a physical raw material can be forged into various tools, CODI uses HKDF to provide the essential raw entropy that can be functionally adapted to any of the three cryptographic domains without requiring the coin to exist in multiple mathematical states at once.

A key advantage of this structure is its non-destructive nature - the coin is not “lost” in any way- you can use it to encrypt, and after decrypting, you have that coin again!

This system is completely scalable, just like today’s Fiat money: a single of our coins with a bit-length of just 32 be of little value to the user, just as a single penny is hardly good for anything.

But just as pennies can add up to billions of dollars, the same can be said about the entropy in our coins: it adds up!

Why is this important? Modern cryptography uses very different bit-sizes, from 64bits for low-security everyday uses to numbers 2000bits and higher in high-security systems.

Generating a truly secure 3200-bit length (e.g., for post-quantum modules) independently can require seconds, minutes or even hours of intensive computation, depending on the level of security one chooses. Using 100 CODI and HKDF, the same result is achieved faster, and, what is more important, with a higher security and transparency!

But, you might ask, can many little numbers really make a new big number, that is as equally secure and has the same properties for cryptography?

And also, does such an intersecting set for the three functions realistically exist in the first place?

Math shows us that this is possible, feasible, robust and fast!

3. The mathematical foundation of CODI: HKDF and Sieving

Critics might argue that finding a single number satisfying the structural requirements for Elliptic Curve Cryptography (ECC), Lattice-Based Cryptography, and Hash-functions simultaneously is mathematically impossible due to conflicting constraints. This would be true if we searched for these properties in parallel.

However, CODI utilizes a hierarchical approach to prove the existence of this intersection.

3.1. How CODI finds the number for one of its coins

Instead of searching for three conflicting structures, CODI filters numbers sequentially:

1. The Primary Filter (Scarcity): First, the protocol searches for a "Safe Prime" (x = 2q + 1). This is the mathematically hardest constraint and provides the scarcity (Proof-of-Work) and the direct utility for ECC private keys.
2. The Secondary Filter (Quality): Once a Safe Prime is found, it is treated as a raw bit-string. This string is tested against statistical requirements (such as NIST SP 800-22) to ensure it has high entropy. A Safe Prime, despite its algebraic structure, appears statistically random in its binary representation.
3. The Universal Seed: Because the number passes the statistical tests, it can serve as a perfect "Seed" for Lattice-based algorithms (like Kyber) and Hash-functions via HKDF.

Therefore, we do not need a number that "is" a Lattice-parameter geometrically; we need a Safe Prime that serves as a certified, high-entropy seed.

3.1.1. Formal Mathematical Definitions

To rigorously define the CODI Standard, we define the search space S and seek a value x such that all three validity conditions (Phi) return TRUE:

Phi_ECC (x) AND Phi_Lattice (x) AND Phi_Hash (x) = TRUE

Definition A: ECC-Suitability (Phi_ECC) The value x must be a Safe Prime to ensure resistance against small-subgroup attacks in Elliptic Curve Cryptography.
Formula: is_prime(x) AND is_prime((x - 1) / 2) = TRUE

Definition B: Lattice-Compatibility (Phi_Lattice) To serve as a seed for Module-LWE schemes (Post-Quantum), the bit-structure of x must exhibit high spectral entropy. We apply a Key Derivation Function (HKDF) and verify the output against the NIST Statistical Test Suite. Formula: NIST_Test(HKDF(x, Salt_Lattice)) > Threshold_Alpha

Definition C: Hash-Seeding Quality (Phi_Hash) The number must possess maximum Min-Entropy. We require the Hamming Weight (Popcount) of the binary representation to be close to 50% of the bit-length (L) to prevent sparse-vector weaknesses.

Formula: ABS(Popcount (x) - (L / 2)) < Epsilon

Probability & Scarcity The probability P (x) of finding a valid CODI coin is the product of the probabilities of these filters. Since Safe Primes are sparse, the computational effort (Work) required to find x defines the intrinsic digital value.

3.2. How single coins of CODI are aggregated

The final cryptographic key (K_final) is derived through an iterative filtering process:

K_final = Sieving(HKDF(K_master, info + j, L))

Where:

- K_master: The aggregated entropy from CODI tokens.
- info: The context parameter (e.g., "Lattice-Key-Gen").
- j: A deterministic counter (Nonce) starting at 0.
- L: The target bit-length (e.g., 3,200 bits).

The process repeats (j = j + 1) until the output satisfies the property test:
Test(K_final) == TRUE

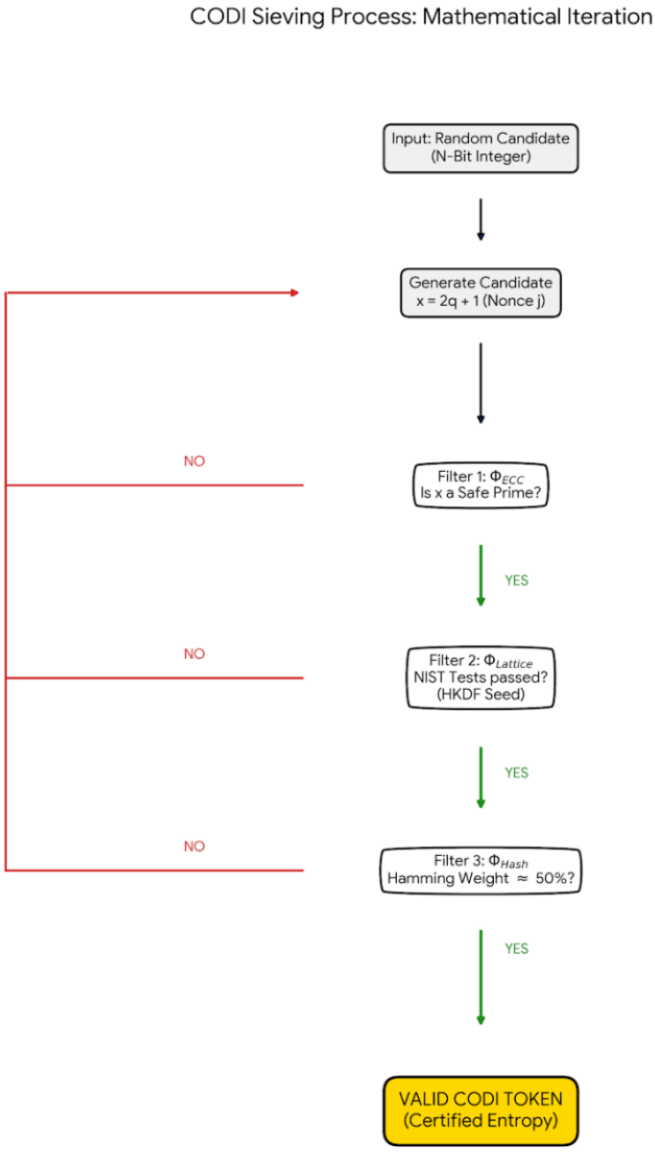
Or put another way:

Input: Aggregated_Entropy (from n CODI tokens)
Output: Validated_Key (L-bit cryptographic parameter)

1. Let j = 0
2. Define Context_String (e.g., "Lattice", "Prime", or "Hash")
3. REPEAT:
   a. Candidate = HKDF_Expand(Aggregated_Entropy, Context_String + j, L)
   b. IF Property_Test(Candidate) == PASSED:

RETURN Candidate

c. ELSE:
j = j + 1 UNTIL Validated_Key is found



So this is the value of our coins! It will very likely be a value in a hundred years, even in a thousand ones.

4. The Devil's Advocate: do we really need CODI?

In philosophy and science, there is the valuable tradition of stating the potential criticism to one's own theory or proposal, in the most clear and "sharp" manner possible.

This is beautiful, as it incorporates the valid points of criticism (which every theory and every project has!) and addresses them in a fair manner!

People we deeply respect, like Charles Darwin, Karl Popper and Thomas of Aquin, did just that in their works and we are proudly following this tradition!

4.1. The "Efficiency" Objection

Critique: Modern smartphones and servers generate entropy in microseconds. Why use a decentralized network for something that is "free and fast" locally?

The CODI Rebuttal: Local entropy is fast, but it is a "Black Box". Users must blindly trust hardware manufacturers and OS-level generators which lack transparent verification. CODI does not compete on raw speed for trivial tasks; it provides Verified Sovereignty.

CODI is the "digital silver coin" of the 21st century. In the ancient world, a merchant could bite a silver coin to instantly verify its purity and value. CODI brings this physical certainty to the digital age: Our mathematical filters (Safe Prime & NIST-Tests) are the "bite test" for the modern user.

While other systems ask you to trust a hidden chip, CODI allows you to verify the "purity" of your entropy yourself, at any time.

It is the only cryptographic system where you don't just see the "silver" - you can verify the soul of the number.

By using Zero-Knowledge Proofs (ZKP), CODI ensures that entropy meets elite mathematical standards before it enters the system, eliminating the need to trust proprietary hardware that may contain undocumented backdoors.

4.2. The "Universal Number" Paradox

Critique: Cryptographic standards like Kyber or Dilithium use simple random seeds. They do not require "multi-domain" numbers optimized for Lattice, ECC, and Hash functions simultaneously.

The CODI Rebuttal: Current "Crypto-Agility" assumes that swapping algorithms is seamless. However, history shows that mathematical breakthroughs can happen unexpectedly. CODI's Multi-Domain certified entropy acts as a high-purity, "digital raw material". By providing a seed that is demonstrably strong across three distinct mathematical fields, it provides a unique insurance policy: even if one cryptographic

domain is compromised, the underlying entropy remains robust for the others, facilitating a safer and more stable migration.

4.3. The "Open Source Trust" Argument

Critique: Public libraries like OpenSSL are community-audited and transparent. Why distrust them?

The CODI Rebuttal: Open-source does not equal immunity. Vulnerabilities (e.g., Heartbleed or XZ-Utils) prove that even widely used code can harbor flaws for years. CODI moves the trust anchor from human review (code) to mathematical proof (ZKP)!

While code can be manipulated, a ZKP-verified coin is a deterministic mathematical fact. CODI provides an independent, state-agnostic layer of security that complements existing libraries rather than just replacing them.

4.4. The "Trust Starvation" Reality

Critique: Modern Operating Systems are excellent at avoiding entropy depletion.

The CODI Rebuttal: This holds for consumer devices but fails at the infrastructure level. High-load environments (cloud servers, massive IoT arrays) can face "Trust Starvation" during peak demand. Unlike the “Entropy Starvation” of earlier times, the problem is no longer creating enough entropy, but creating entropy with enough quality!

CODI acts as a Global Entropy Reservoir, allowing systems to "inject" pre-verified, high-performance entropy without taxing local hardware resources. It delivers a scalable solution for the immense security requirements of a fully digitized global economy.

4.5. The "Computational Velocity" Advantage in High-Security Primes

Critique: Standard libraries generate keys in milliseconds. The claim of "much faster" seems exaggerated for modern hardware.

The CODI Rebuttal: Local generation’s perceived speed applies only to "simple" random seeds used in standard post-quantum cryptography (PQC). However, high-assurance systems often require numbers with specific mathematical properties - such as large "Safe Primes" (e.g., 3200-bit to 4096-bit) or complex lattice structures that must simultaneously satisfy multiple security tests.

- The "Needle in the Haystack" Problem: Finding a 3200-bit number that satisfies Lattice, Hash, and ECC properties concurrently is an exponentially difficult "Sieving" task that can take minutes or even hours of intensive local CPU cycles.
- Pre-Certified Velocity: CODI miners have already performed this "brute-force" mathematical labor. By aggregating CODI coins, a user starts with "pre-certified" high-quality entropy.
- The Result: Instead of the local device performing millions of trial-and-error tests ($j = j + 1$), it simply verifies a ZKP and runs a lightweight HKDF expansion. In these

high-security scenarios, CODI transforms an "intensive computation" into a "simple verification," achieving the cited „much faster“ reduction in local processing time.

4.6. Conclusion: The Value of CODI

The value of CODI is perhaps best illustrated by a comparison with silver: silver coins were valuable not because everybody used silverware or silver jewelry, far from it!

They were valuable to everybody because everyone knew that some people were using silver in this way, and that was enough for universal value!

5. The practical aspects of CODI

5.1. Security

An elegant feature of Cotidianus Digitalis lies in the complete unification of intrinsic value and security.

Each coin represents a unique number that is directly usable in lattice-based, hash-based, and elliptic curve cryptography – this number is the sole source of the coin’s real, lasting utility and intrinsic value.

At the same time, this very number forms the foundation of the coin’s authenticity proof. During minting, the miner generates a zero-knowledge proof (ZKP) that demonstrates to the network:

- “This coin is backed by a number possessing all three required cryptographic properties,”
  without ever revealing the number itself.

Thus, the proof of authenticity is not a separate, artificial mechanism, but identical with the proof of value. *The coin is secure because it is valuable – and valuable because it is secure*.

This construction is made possible by zero-knowledge proofs, specifically modern succinct non-interactive arguments of knowledge (zk-SNARKs or zk-STARKs), which allow the prover to convince the verifier of the correctness of a statement (here: the number’s required properties) while revealing no information beyond the statement’s truth.

Cotidianus Digitalis thereby achieves a cryptographic ideal: value and security are not merely linked – they are one and the same!

5.2. Minting

The key to absolutely every currency, digital or not, is how and by whom it is or can be minted.

If it is too easy to mint, inflation is inevitable!

If there is a central power minting it, loss of freedom is! (And inflation also comes with it!)

If it is capped or impossible to mint, deflation will make it completely useless for everyday life over time!

So how do we go about this?

The minting process in Cotidianus Digitalis is designed to generate new coins in a decentralized, secure, and adaptive manner.

Each coin embodies a unique number with the three core cryptographic properties (lattice-based, hash-based, and elliptic curve cryptography). Miners search for qualifying numbers and submit a zero-knowledge proof (ZKP) to the network, verifying the number's properties without revealing it. Upon successful validation, the new coin is issued.

Minting is tied to a vault mechanism that encourages long-term holding and provides yield through interest. *Vaults are inherent to the coins themselves – no separate external structure is required! Users can seamlessly fuse multiple coins into a single vault entity, aggregating them for the desired commitment period and size*.

5.2.1. Vault Architecture

The Yield in the CODI Vault is determined by your "Work" (Bits) and your commitment (Time and Volume).

5.2.1.1. The Base Rate (The 100-Bit Rule)

The Base Rate is the starting point for your interest. It is calculated by the amount of work you invest in your Vault.

- Step A: We look at the total Bits you produced for all coins in your Vault.
- Step B: We divide these Bits by 100. This gives us your "Minted Units".
- Step C: We compare these units to the total number of CODI in your Vault to get the Base Rate percentage.

5.2.1.2. The Vault Equality Rule

To keep the system reasonable, all coins in a Vault must be brought up to the same quality. If you have one coin with a high Bit-Depth (e.g., 50 Bits), all other coins in that Vault must be minted to at least that same level before they can generate interest. This prevents "Super-Coins" from distorting the system.

Example:

- You have 10,000 CODI in the Vault.
- You produce 100,000 Bits (by increasing the bit- depth of your coins).

- Divide the produced bits by 100 and then see what interest rate the coins in the vault would produce for that number. That will be your Base Rate, in this case 10%. (As 100,000 divided by 100 is thousand, and you would need a 10% interest rate to produce this with 10000 coins in the vault)

5.2.1.3. The Multipliers (Time & Volume)

Once the Base Rate is determined, we apply the multipliers for Duration and Mass.

The Final Yield Formula: Final_Yield = Base_Rate * Duration_Multiplier * Volume_Multiplier

A. Duration Multiplier (D): Rewards the length of your commitment (t = months). You can choose any duration from 6 months to infinity. Formula: D = (t / 6) ^ 0.7

B. Volume Multiplier (V): Rewards the amount of CODI you hold (M = Amount). Formula: V = (M / 1000) ^ 0.05

Practice Examples: The Impact of Work (Bits)

To understand how the Vault rewards both capital and labor, let's look at Mr. Miller in two different scenarios. In both cases, he puts 16,000 CODI into the Vault for 14 months.

Common Multipliers for both examples:

- Duration Multiplier (D): (14 / 6) ^ 0.7 = 1.81
- Volume Multiplier (V): (16,000 / 1,000) ^ 0.05 = 1.15
- Combined Multiplier (D * V): 1.81 * 1.15 = 2.08

Scenario A: Mr. Miller the "Hard Worker" (+5 Bits)

In this case, Mr. Miller spends more energy to significantly increase the quality of his coins.

- Step 1 (Work): 16,000 coins * 5 Bits = 80,000 total Bits.
- Step 2 (Base Rate): 80,000 Bits / 100 = 800 units.
- Base Rate Percentage: 800 / 16,000 = 5.0%
- Final Calculation: 5.0% (Base) * 2.08 (Multipliers) = 10.4% Total Yield.

  With this work, Mr. Miller has increased the security and thus the value of the coins by the factor of 32! More than enough for every advancement in technology.

Scenario B: Mr. Miller the "Minimum Effort" (+1 Bit)

In this case, Mr. Miller only does the bare minimum required to keep his coins updated.

- Step 1 (Work): 16,000 coins * 1 Bit = 16,000 total Bits.
- Step 2 (Base Rate): 16,000 Bits / 100 = 160 units.
- Base Rate Percentage: 160 / 16,000 = 1.0%
- Final Calculation: 1.0% (Base) * 2.08 (Multipliers) = 2.08% Total Yield.

With this little effort, Mr. Miller has just doubled the security of his coins in 14 months, roughly the pace of “Moore’s Law“!

5.2.2. Why splitting the Vault is a mistake (Anti-Split Logic)

The Volume Multiplier (V) is "super-inverse." This means the larger the amount in a single Vault, the higher the multiplier.

- If Mr. Miller keeps his 16,000 CODI together, his V-factor is 1.15.
- If he splits them into 16 separate Vaults of 1,000 CODI each, his V-factor drops to 1.00 for every single one.

By splitting, he would lose about 15% of his potential gains immediately. The protocol mathematically punishes fragmentation and rewards the consolidation of wealth into stable, large-scale nodes. This ensures the network remains strong and unified.

5.3. Summary of Rules

- No Free Lunch: If you produce 0 bits, your Base Rate is 0%, and you receive 0 interest.
- Fixed Contracts: Vaults are fixed for the chosen time (from 6 months upwards). No extensions.
- Uniform Quality: The highest bit-depth in your Vault sets the requirement for all other coins in that same Vault.
- Concrete Anchor: The "100-Bit Rule" is a constant and will never change.
- The bit-length of the coins constantly increases and thus their value and security!

Also, they stay ahead of the inevitable progress in computational power of our hardware!

5.4. The Emergency Exit (The Burn-Rate)

The CODI Vault is designed for commitment. However, if a user needs to access their capital before the contract ends, they can use the Emergency Exit. This triggers a "Burn," where a small percentage of the principal is destroyed.

5.4.1. The Logic of the Burn

The Burn-Rate serves two main purposes:

- Money Supply Regulation: It prevents sudden floods of coins into the market, protecting the value for all other holders.

- Anti-Speculation: It discourages short-term traders from using the Vault as a playground, ensuring that only serious, long-term participants benefit.

The rule is straightforward: Loyalty is rewarded. The longer your original commitment was, the lower your penalty becomes.

5.4.2. The Burn Formula

The penalty is calculated based on the planned duration (t) of the Vault in months. Formula: Burn_Rate = 0.05 / (t / 6)

(Note: Since the minimum Vault duration is 6 months, the maximum penalty is capped at 5% for the shortest possible Vault. As time increases, the penalty drops significantly.)

Practice Examples:

Example A: Short-Term Commitment (7 Months) A user locks their CODI for only 7 months but needs to exit early.

- Calculation: 0.05 / (7 / 6) = 0.05 / 1.16
- Result: 4.29% Burn Penalty.
- Logic: Because the commitment was very short, the "protection fee" for the network is high.

Example B: Long-Term Commitment (27 Months) A user planned to stay for 27 months but decides to exit early.

- Calculation: 0.05 / (27 / 6) = 0.05 / 4.5
- Result: 1.1% Burn Penalty.
- Logic: The user showed a much stronger intent to support the network, so the penalty is lower.

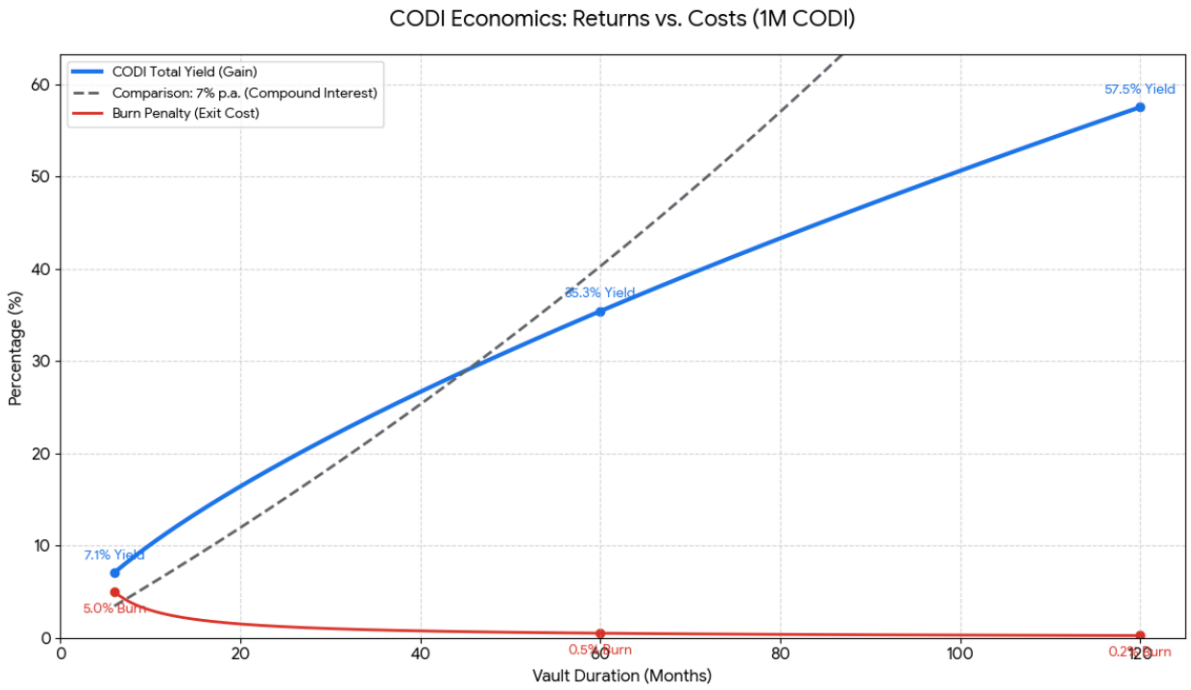
Example C: The Visionary (120 Months) A user committed to 10 years (120 months).

- Calculation: 0.05 / (120 / 6) = 0.05 / 20
- Result: 0.25% Burn Penalty.
- Logic: At this stage, the penalty is almost symbolic (less than 1%), as the user has proven maximum loyalty to the ecosystem.

5.4.3. Summary of the Burn

- Minimum Duration: You must plan for at least 6 months.

- Fixed Penalty: The penalty is fixed at the moment you create the Vault, based on



your planned time.
- Fair Exit: Even in an emergency, only a small fraction of your coins are lost.

5.5. Considerations for the amount of money in CODI

As you see, it is rather easy to increase the amount of CODI and thus, the amount of money in existence.

This stems from a key insight: inflation is completely self-regulating in CODI, while deflation could kill its usability!

The world-economy can sometimes grow in numbers unimaginable, either by political shifts like the rise of China or the end of the Cold War or by technical breakthroughs like the steam-engine or the internet! Currency and the amount of money must expand accordingly, otherwise deflation makes the currency unsuitable for the smaller goods of everyday-life. We constructed the CODI-vault with this aim in mind.

Inflation, on the other hand, will never be truly a problem in CODI, as people will stop minting if the price of electricity, processing- capacity or simply time exceeds the gains of newly minted CODI.

Unlike in Fiat money, where a central bank can print till the end of time or hyper-inflation, the decentralized nature of CODI keeps the amount of money always in check!

6. Small, but important details

There are lots of things to consider when it comes to a new project, here we demonstrate that CODI addresses them all!

6.1. What will be the initial size of the number used in CODI?

This will be determined in the implementation phase of the project!

As of now, we consider numbers in the size range 32-bit, but other sizes outside this range are perfectly feasible.

6.2. How many CODI will be launched?

CODI is meant as a digital everyday currency for everyone worldwide, which means that a lot of them have to be around for the start!

We plan to launch at least 2 billion CODI in the beginning, but that number is not written in stone!

6.3. How does CODI ensure that each “coin” has a unique number?

To guarantee that no number is used more than once, Cotidianus Digitalis (CODI) employs a decentralized, on-chain registry of cryptographic hashes.

When a miner submits a new coin for minting, they provide:

- the zero-knowledge proof verifying the number’s required properties, and
- the SHA-hash of the secret number itself.

The network checks whether this hash already exists in the global registry. If it does, the minting attempt is rejected. If the hash is new and the ZKP is valid, the coin is accepted, the hash is irreversibly added to the registry.

The secret number remains forever hidden – only its hash is stored publicly. This mechanism is fully decentralized, transparent, and enforced by every node, preventing duplicates without compromising privacy or requiring any trusted party.

6.4. How many coins for the Founder and his team?

Given the number of problems CODI addresses, we think a 18% share for us is fair; the exact number may vary, of course.

To ensure the long-term stability of CODI and to align the interests of the founding team with those of every "Free Citizen" in our network, we implement a strict Founder’s Vesting Protocol.

While a 18% share is reserved for the creators to compensate for the years of development, these coins are not accessible at launch. Instead, they are subject to the following "Proof of Loyalty":

- The 12-Month Cliff: For the first year after the Genesis-Mint, zero coins from the founder's share can be moved or sold. This ensures that the team's sole focus remains on the implementation and growth of the ecosystem.
- Linear Release: After the initial 12-month cliff, the coins will be released gradually at a rate of 2% per month over the following 50 months.
- The "Lead by Example" Rule: Just like our users in the Vaults are rewarded for their "Duration of Commitment", the founders' coins are mathematically locked within the protocol. This prevents any "sudden floods" of coins into the market, echoing our principle of Money Supply Regulation.
- Transparency: Every release is recorded on the decentralized on-chain registry, making the founders' commitment as verifiable as the ZKP of a single CODI coin.

By moving the trust anchor from Human Promises to Mathematical Proof, we ensure that the team stays "in the boat" until CODI has reached its goal of being a worldwide currency.

6.5. Will the testing of CODI coins be done with every transaction?

No, CODI coins do not require a full zero-knowledge proof verification on every transaction.

The computationally intensive cryptographic verification, the zero-knowledge proof that confirms the secret number satisfies all three required properties, is performed only once, during the minting process. Upon successful validation, the network issues a lasting digital signature that certifies the coin's authenticity. This signature is stored on-chain and permanently attached to the coin.

In subsequent transactions, such as everyday purchases like buying an ice cream, only this lightweight digital signature needs to be verified. This is a standard cryptographic operation that completes in milliseconds on any device, with no need to recompute the zero-knowledge proof or inspect the secret number.

This design enables CODI to deliver transaction speeds and costs comparable to conventional digital payment systems, while preserving the strongest possible cryptographic guarantees at the point of issuance.

6.6. How will CODI be used in daily life?

Well, you choose: prepaid debit cards, ordinary debit cards, credit cards, and of course smartphone apps and online banking! Whatever you wish!

Thus, there should be no application for which the ordinary citizen can't use CODI!

6.7. What regulations apply to CODI?

As CODI is developed within the European Union (Frankfurt am Main), we are committed to aligning with the Markets in Crypto-Assets (MiCA) regulation. We categorize CODI primarily as a Utility Token, providing intrinsic value through certified entropy. By

proactively addressing these standards, CODI ensures legal certainty for institutional partners and long-term stability within the European financial ecosystem.

6.8. What about governments? Won't they oppose CODI?

Well, that might be! Governments love power, and Free Citizens love their freedom from that power! Conflicts are inevitable and will probably occur till the sun explodes!

Thus, while we expect some governments and their bureaucracies to hate CODI, we also think that the wish for a better monetary system will allow CODI to thrive!

Struggle is a part of life, but easy to cope with if what you fight for is worth it!

7. The initial release in the market and the potential Catch-22 of CODI

Money must show its value in everyday transactions - if shops and pubs don't accept it, people will not use it. If people will not use it, shops and pubs will see no reason to accept it!

CODI can overcome this initial problem rather easily by targeting the people most in need of it - frequent users of cryptography with the need for long-term, extremely strong security.

Five examples of such users are:

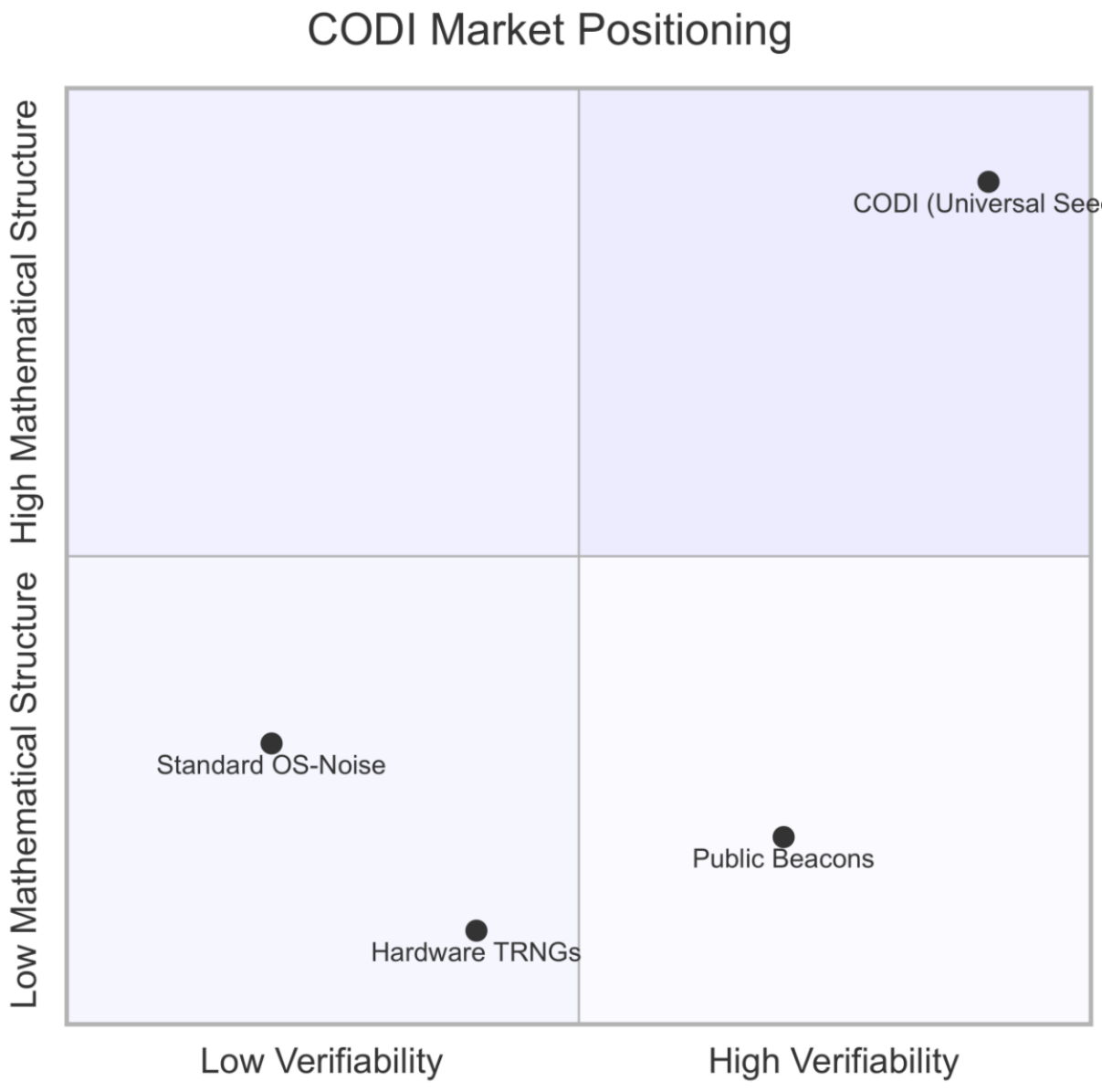
1. Banks and payment apps (like PayPal, Revolut, or your bank's app)
   They protect online transfers, card payments, and account logins. They use very long keys (often 4096-bit or more) because a single breach could cost millions and affect thousands of customers.
2. Cloud storage providers (like Dropbox, Google Drive, or iCloud)
   They encrypt your photos, documents, and backups. High bit lengths ensure that even if someone steals the data, it stays unreadable for decades.
3. Secure messaging and email services (like WhatsApp, Signal, or ProtonMail)
   End-to-end encryption keeps your chats and emails private. They rely on strong keys so that no one – not even the company – can read your messages.
4. Online shopping platforms (like Amazon, Zalando, or any web shop)
   They secure your credit card details and orders during checkout. Strong cryptography prevents fraud and protects millions of transactions every day.
5. VPN and privacy services (like NordVPN or ExpressVPN)
   They hide your internet traffic and protect you on public Wi-Fi. Long, high-entropy keys make sure your browsing stays private, even against powerful attackers.

These companies handle sensitive data for millions of ordinary users every day, so they need the strongest possible encryption – and that creates a constant demand for reliable, high-quality cryptographic building blocks.

And, given the possibility of an independent proof every time the user wishes to secure himself, we expect a huge *Veblen effect*! After all, if your competitor and neighbor has the latest and greatest AND independent security, you should keep up with it, right?

Thus, CODI will probably effortlessly find its first customers and users - and luckily, these are Big Players in today's economy!

With such a starting point, expansion shouldn't be too difficult.



8. Prospects

We think CODI is the future of currency and we hope that we have provided sufficient evidence for this -admittedly!- quite strong claim.

A useable, valuable, stable digital currency that allows transactions across borders and decades!

It addresses numerous challenges of today's economics, warranting it being called revolutionary!

Thus, we think it is worth investing time, work and money into it!

And there will be a huge reward for the Early Adopters: since minting CODI is very easy if the bit number on a coin is as low as 32, early investors will be able to harvest huge interest rates in a very short period of time!

We would love to build a team that creates CODI for the real world and welcome any contributions you can make!

9. Legal notice (Imprint)

Author: Ludwig Staab

Kriegkstraße 31

60326 Frankfurt am Main Germany

Contact:

E-Mail: cotidianus-digitalis@protonmail.com

Tel.: +49 179 9133395

Website: www.cotidianus-digitalis.com

Frankfurt am Main, January 2026